日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　７月１１日

出願番号
Application Number: 特願２００３－１９５６２６

[ST. 10/C]: [ＪＰ２００３－１９５６２６]

出願人
Applicant(s): 株式会社リコー

２００３年１２月　５日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３１００６８０

【書類名】　特許願

【整理番号】　0300734

【提出日】　平成15年 7月11日

【あて先】　特許庁長官　　太田　信一郎　殿

【国際特許分類】　G06F 12/00

【発明の名称】　プログラム改ざん検証方法、カプセル化文書構造、記憶媒体、カプセル化文書作成装置、改ざん検証装置、カプセル化文書作成処理プログラム、これを記憶する記憶媒体、起動プログラム及びこれを記憶する記憶媒体

【請求項の数】　32

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内

【氏名】　長谷川　雄史

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内

【氏名】　鈴木　明

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内

【氏名】　小出　雅巳

【特許出願人】

【識別番号】　000006747

【氏名又は名称】　株式会社リコー

【代表者】　桜井　正光

【代理人】

【識別番号】　100101177

【弁理士】

【氏名又は名称】　柏木　慎史

【電話番号】　03(5333)4133

【選任した代理人】
　【識別番号】　100102130
　【弁理士】
　【氏名又は名称】　小山　尚人
　【電話番号】　03(5333)4133
【選任した代理人】
　【識別番号】　100072110
　【弁理士】
　【氏名又は名称】　柏木　明
　【電話番号】　03(5333)4133
【手数料の表示】
　【予納台帳番号】　063027
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9808802
　【包括委任状番号】　0004335
【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　プログラム改ざん検証方法、カプセル化文書構造、記憶媒体、カプセル化文書作成装置、改ざん検証装置、カプセル化文書作成処理プログラム、これを記憶する記憶媒体、起動プログラム及びこれを記憶する記憶媒体

【特許請求の範囲】

【請求項１】　文書上での表現実体となる文書情報ファイルと、当該文書情報ファイルを表現実体化させる動作プログラムファイルとが少なくともカプセル化されているカプセル化文書ファイルにおける前記動作プログラムファイルの改ざん検証処理を情報処理部により実行するプログラム改ざん検証方法であって、

前記文書情報ファイルの表現実体化に際して前記カプセル化文書ファイル内の前記動作プログラムファイルの特徴量を算出するステップと、

予め保持しておいた前記動作プログラムファイルの暗号化特徴量を復号化するステップと、

復号化した前記動作プログラムファイルの特徴量と算出された前記動作プログラムファイルの特徴量とを比較するステップと、

特徴量が一致しない場合に、前記動作プログラムファイルによる前記文書情報ファイルの表現実体化を制限するステップと、

を具備するプログラム改ざん検証方法。

【請求項２】　文書上での表現実体となる文書情報ファイルと、当該文書情報ファイルを表現実体化させる動作プログラムファイルの保存位置を示す位置情報とが少なくともカプセル化されているカプセル化文書ファイルにおける前記動作プログラムファイルの改ざん検証処理を情報処理部により実行するプログラム改ざん検証方法であって、

前記文書情報ファイルの表現実体化に際して前記カプセル化文書ファイル内に保持された位置情報に存在する前記動作プログラムファイルの特徴量を算出するステップと、

予め保持しておいた前記動作プログラムファイルの暗号化特徴量を復号化するステップと、

復号化した前記動作プログラムファイルの特徴量と算出された前記動作プログ

ラムファイルの特徴量とを比較するステップと、

特徴量が一致しない場合に、前記動作プログラムファイルによる前記文書情報ファイルの表現実体化を制限するステップと、

を具備するプログラム改ざん検証方法。

【請求項３】　各種ファイルで構成されるファイル群と、

このファイル群を構成する所定のファイルに関する暗号化された特徴量を保持する特徴量保持ファイルと、

をカプセル化手段によってカプセル化したカプセル化文書構造。

【請求項４】　文書上での表現実体となるコンテンツ情報である文書情報ファイルと、

この文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルと、

この動作プログラムファイルに関する暗号化された特徴量を保持する特徴量保持ファイルと、

をカプセル化手段によってカプセル化したカプセル化文書構造。

【請求項５】　文書上での表現実体となるコンテンツ情報である文書情報ファイルと、

この文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルの保存位置を示す位置情報と、

前記動作プログラムファイルに関する暗号化された特徴量を保持する特徴量保持ファイルと、

をカプセル化手段によってカプセル化したカプセル化文書構造。

【請求項６】　文書上での表現実体となるコンテンツ情報である文書情報ファイルと、

この文書情報ファイルを表現実体化させる動作プログラムであり、特徴量が外部に保持されている動作プログラムファイルと、

をカプセル化手段によってカプセル化したカプセル化文書構造。

【請求項７】　文書上での表現実体となるコンテンツ情報である文書情報ファイルと、

この文書情報ファイルを表現実体化させる動作プログラムであり、特徴量が外部に保持されている動作プログラムファイルの保存位置を示す位置情報と、
をカプセル化手段によってカプセル化したカプセル化文書構造。

【請求項８】　前記特徴量保持ファイルには、前記文書情報ファイルに関する暗号化された特徴量も保持されている、
請求項３ないし５の何れか一記載のカプセル化文書構造。

【請求項９】　前記特徴量保持ファイルには、前記動作プログラムファイルに関する暗号化された特徴量に対応付けられて前記暗号化された特徴量を復号化する復号化鍵情報が保持されている、
請求項３ないし５の何れか一記載のカプセル化文書構造。

【請求項１０】　前記特徴量保持ファイルには、前記動作プログラムファイルに関する暗号化された特徴量に対応付けられて前記暗号化された特徴量を復号化する復号化鍵情報の保存位置を示す位置情報が保持されている、
請求項３ないし５の何れか一記載のカプセル化文書構造。

【請求項１１】　各動作プログラムファイル毎に異なる前記復号化鍵情報が対応付けられている、
請求項９または１０記載のカプセル化文書構造。

【請求項１２】　前記動作プログラムファイルに関する特徴量は、公開鍵暗号方式により暗号化されている、
請求項３ないし１１の何れか一記載のカプセル化文書構造。

【請求項１３】　前記復号化鍵情報は、第三者認証局により署名暗号化されている、
請求項１２記載のカプセル化文書構造。

【請求項１４】　前記動作プログラムファイルに関する特徴量は、秘密鍵暗号方式により暗号化されている、
請求項３ないし１１の何れか一記載のカプセル化文書構造。

【請求項１５】　前記動作プログラムファイルの改ざん検証を実行する特徴量検証プログラムファイルをカプセル化手段によってカプセル化した、
請求項３ないし１４の何れか一記載のカプセル化文書構造。

【請求項１６】　請求項３ないし１５の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを格納した、
記憶媒体。

【請求項１７】　文書上での表現実体となるコンテンツ情報である文書情報ファイルを取得する文書情報ファイル取得手段と、

コンピュータにより解釈、実行されて、前記文書情報ファイル取得手段により取得された前記文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルを取得する動作プログラムファイル取得手段と、

前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、

この特徴量算出手段により算出した前記動作プログラムファイルの特徴量を暗号化鍵情報で暗号化し、特徴量保持ファイルに保存する特徴量保持ファイル生成手段と、

前記文書情報ファイルと前記動作プログラムファイルと前記特徴量保持ファイルとを単一の文書としてカプセル化するカプセル化手段と、
を備えるカプセル化文書作成装置。

【請求項１８】　前記文書情報ファイルの特徴量を算出する文書情報特徴量算出手段を備え、

この文書情報特徴量算出手段により算出した前記文書情報ファイルの特徴量も暗号化鍵情報で暗号化し、前記特徴量保持ファイルに保存する、
請求項１７記載のカプセル化文書作成装置。

【請求項１９】　請求項３ないし１５の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを読み込む読込み手段と、

この読込み手段により読み込まれた前記カプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、前記動作プログラムファイルの改ざん検証を実行する改ざん検証手段と、
を備える改ざん検証装置。

【請求項２０】　前記改ざん検証手段は、

前記読込み手段により読み込まれた前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量を復号化す

る復号化手段と、

前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、

この特徴量算出手段により算出された前記動作プログラムファイルの特徴量と前記復号化手段により復号化された前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、

を備える請求項１９記載の改ざん検証装置。

【請求項２１】　前記改ざん検証手段は、

前記読込み手段により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、

この特徴量算出手段により算出された前記動作プログラムファイルの特徴量と起動プログラム内の前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、

を備える請求項１９記載の改ざん検証装置。

【請求項２２】　前記改ざん検証手段は、

前記読込み手段により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、

この特徴量算出手段により算出された前記動作プログラムファイルの特徴量を暗号化する暗号化手段と、

この暗号化手段により暗号化された前記動作プログラムファイルの暗号化特徴量と前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、

を備える請求項１９記載の改ざん検証装置。

【請求項２３】　前記改ざん検証手段は、

前記読込み手段により読み込まれた前記カプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出する特徴量算出手段と、

この特徴量算出手段により算出された前記特徴量検証プログラムファイルの特

徴量と起動プログラム内の前記特徴量検証プログラムファイルの特徴量とに基づいて前記特徴量検証プログラムファイルを実行するか否かを判定する判定手段と、

この判定手段により前記特徴量検証プログラムファイルを実行すると判定された場合、前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、

を備える請求項１９記載の改ざん検証装置。

【請求項２４】　コンピュータにインストールされ、

文書上での表現実体となるコンテンツ情報である文書情報ファイルを取得する文書情報ファイル取得機能と、

コンピュータにより解釈、実行されて、前記文書情報ファイル取得機能により取得された前記文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルを取得する動作プログラムファイル取得機能と、

前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、

この特徴量算出機能により算出した前記動作プログラムファイルの特徴量を暗号化鍵情報で暗号化し、特徴量保持ファイルに保存する特徴量保持ファイル生成機能と、

前記文書情報ファイルと前記動作プログラムファイルと前記特徴量保持ファイルとを単一の文書としてカプセル化するカプセル化機能と、

をコンピュータに実行させるカプセル化文書作成処理プログラム。

【請求項２５】　前記文書情報ファイルの特徴量を算出する文書情報特徴量算出機能をコンピュータに実行させ、

この文書情報特徴量算出機能により算出した前記文書情報ファイルの特徴量も暗号化鍵情報で暗号化し、前記特徴量保持ファイルに保存する、

請求項２４記載のカプセル化文書作成処理プログラム。

【請求項２６】　請求項２４または２５記載のカプセル化文書作成処理プログラムを記憶する記憶媒体。

【請求項２７】　請求項３ないし１５の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを読み込む読込み機能と、

この読込み機能により読み込まれた前記カプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、前記動作プログラムファイルの改ざん検証を実行する改ざん検証機能と、
をコンピュータに実行させる起動プログラム。

【請求項２８】　前記改ざん検証機能は、

前記読込み機能により読み込まれた前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量を復号化する復号化機能と、

前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、

この特徴量算出機能により算出された前記動作プログラムファイルの特徴量と前記復号化機能により復号化された前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、
をコンピュータに実行させる請求項２７記載の起動プログラム。

【請求項２９】　前記改ざん検証機能は、

前記読込み機能により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、

この特徴量算出機能により算出された前記動作プログラムファイルの特徴量と起動プログラム内の前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、
をコンピュータに実行させる請求項２７記載の起動プログラム。

【請求項３０】　前記改ざん検証機能は、

前記読込み機能により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、

この特徴量算出機能により算出された前記動作プログラムファイルの特徴量を暗号化する暗号化機能と、

この暗号化機能により暗号化された前記動作プログラムファイルの暗号化特徴量と前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作

プログラムファイルの暗号化特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、
をコンピュータに実行させる請求項２７記載の起動プログラム。

【請求項３１】　前記改ざん検証機能は、

前記読込み機能により読み込まれた前記カプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出する特徴量算出機能と、

この特徴量算出機能により算出された前記特徴量検証プログラムファイルの特徴量と起動プログラム内の前記特徴量検証プログラムファイルの特徴量とに基づいて前記特徴量検証プログラムファイルを実行するか否かを判定する判定機能と、

この判定機能により前記特徴量検証プログラムファイルを実行すると判定された場合、前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、
をコンピュータに実行させる請求項２７記載の起動プログラム。

【請求項３２】　請求項２７ないし３１のいずれか一記載の起動プログラムを記憶する記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、プログラム改ざん検証方法、カプセル化文書構造、記憶媒体、カプセル化文書作成装置、改ざん検証装置、カプセル化文書作成処理プログラム、これを記憶する記憶媒体、起動プログラム及びこれを記憶する記憶媒体に関する。

【０００２】

【従来の技術】

現在、コンピュータは各種の情報を表示、作成する道具として一般的である。このような情報は、一般的に「電子文書」と呼ばれている。そして、電子文書は、通常、「文書作成アプリケーションプログラム」と呼ばれるコンピュータ上で動作するプログラムによりデジタル情報として作成され、記憶媒体に保存される。また、作成されたデジタル情報はその情報を読込み表示するための「閲覧アプ

リケーションプログラム」と呼ばれるアプリケーションにより表示される。

【０００３】

ここで、電子文書を作成・編集するアプリケーションと閲覧するアプリケーションとは同一のプログラムを使用する場合が多い。代表的なものとしてマイクロソフト社のワード（Microsoft Corporationの登録商標）、エクセル（Microsoft Corporationの登録商標）などがある。

【０００４】

また、使用者はこの電子文書を扱う場合はこれらのアプリケーションプログラムを予めコンピュータの記憶媒体にインストールしておく必要がある。

【０００５】

ところで、電子文書の利用形態を考えると、電子文書を作成する作成者と、閲覧する閲覧者とが異なる場合が多い。つまり、閲覧者は、作成者と同じアプリケーションプログラムを保有していないと電子文書を閲覧することができない。そのため、現在の電子文書を扱う場合、閲覧者は作成された電子文書を閲覧するために、電子文書のデジタル情報のフォーマットを解釈できるアプリケーションプログラムを予め用意する必要がある。

【０００６】

また、作成者と閲覧者が同じアプリケーションプログラムを保有している場合であっても、作成者と閲覧者とのアプリケーションプログラムのバージョンが異なるために、電子文書の表示フォーマットが乱れたり、表示されなくなる場合がある。

【０００７】

そこで、このような問題を解決すべく、本出願人は、特許文献１において、文書のデータ構造として、複数のコンテンツファイルと、それらとそれらの構造を定義した文書構造ファイルと、文書構造ファイルに基づく動作プログラムとを１つのファイルにカプセル化した文書のデータ構造（カプセル化文書）を既に提案している。この特許文献１によれば、電子文書情報に閲覧する動作プログラムをカプセル化することによって、閲覧者は作成者と異なるコンピュータ環境で電子文書を閲覧することが可能になる。

【０００８】

【特許文献１】

特開２００３－０１５９４１公報

【０００９】

【発明が解決しようとする課題】

しかしながら、このように電子文書内にプログラムを保持させることにより新たな問題が生じる。それは、電子文書内のプログラムが閲覧者の意図しない動作を行う可能性があることである。つまり、電子文書内に悪意のあるプログラムを埋込み、閲覧時に動作させることで閲覧者に被害を与えることである。このままではこのような技術を適用した情報を安全に扱うことができない。特に、現在では、文書をインターネット等を使って配布したりすることが一般に行われているため、コンピュータウィルス等の混入が問題になっている。

【００１０】

本発明の目的は、このような問題を解消する新たなデータ構造を提案することである。つまり、コンピュータの動作環境に左右されず、かつ、悪意のあるプログラムの混入を防ぐことを目的とする。

【００１１】

【課題を解決するための手段】

請求項１記載の発明のプログラム改ざん検証方法は、文書上での表現実体となる文書情報ファイルと、当該文書情報ファイルを表現実体化させる動作プログラムファイルとが少なくともカプセル化されているカプセル化文書ファイルにおける前記動作プログラムファイルの改ざん検証処理を情報処理部により実行するプログラム改ざん検証方法であって、前記文書情報ファイルの表現実体化に際して前記カプセル化文書ファイル内の前記動作プログラムファイルの特徴量を算出するステップと、予め保持しておいた前記動作プログラムファイルの暗号化特徴量を復号化するステップと、復号化した前記動作プログラムファイルの特徴量と算出された前記動作プログラムファイルの特徴量とを比較するステップと、特徴量が一致しない場合に、前記動作プログラムファイルによる前記文書情報ファイルの表現実体化を制限するステップと、を具備する。

【００１２】

したがって、動作プログラムファイル全体を暗号化処理せずとも、動作プログラムファイルの特徴量という小さなデータ（２０バイト程度）を暗号化処理するだけで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。これにより、高速にカプセル化文書ファイル内の動作プログラムファイルの改ざん検証が実行できる利便性の高いカプセル化文書ファイルを提供することが可能になる。

【００１３】

請求項２記載の発明のプログラム改ざん検証方法は、文書上での表現実体となる文書情報ファイルと、当該文書情報ファイルを表現実体化させる動作プログラムファイルの保存位置を示す位置情報とが少なくともカプセル化されているカプセル化文書ファイルにおける前記動作プログラムファイルの改ざん検証処理を情報処理部により実行するプログラム改ざん検証方法であって、前記文書情報ファイルの表現実体化に際して前記カプセル化文書ファイル内に保持された位置情報に存在する前記動作プログラムファイルの特徴量を算出するステップと、予め保持しておいた前記動作プログラムファイルの暗号化特徴量を復号化するステップと、復号化した前記動作プログラムファイルの特徴量と算出された前記動作プログラムファイルの特徴量とを比較するステップと、特徴量が一致しない場合に、前記動作プログラムファイルによる前記文書情報ファイルの表現実体化を制限するステップと、を具備する。

【００１４】

したがって、動作プログラムファイル全体を暗号化処理せずとも、動作プログラムファイルの特徴量という小さなデータ（２０バイト程度）を暗号化処理するだけで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。これにより、高速にカプセル化文書ファイル内の動作プログラムファイルの改ざん検証が実行できる利便性の高いカプセル化文書ファイルを提供することが可能になる。

【００１５】

請求項３記載の発明のカプセル化文書構造は、各種ファイルで構成されるファ

イル群と、このファイル群を構成する所定のファイルに関する暗号化された特徴量を保持する特徴量保持ファイルと、をカプセル化手段によってカプセル化した。

【００１６】

したがって、各種ファイルで構成されるファイル群とファイル群を構成する所定のファイルに関する暗号化された特徴量を保持する特徴量保持ファイルとが一元的に管理されていることにより、カプセル化文書ファイルを配布する際に、所定のファイルの暗号化特徴量を復号化するとともに配布された所定のファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中におけるファイルの改ざん検証が可能になる。

【００１７】

請求項４記載の発明のカプセル化文書構造は、文書上での表現実体となるコンテンツ情報である文書情報ファイルと、この文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルと、この動作プログラムファイルに関する暗号化された特徴量を保持する特徴量保持ファイルと、をカプセル化手段によってカプセル化した。

【００１８】

したがって、文書情報ファイルを表現実体化させる動作プログラムファイルが当該文書情報ファイルと一体にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【００１９】

請求項５記載の発明のカプセル化文書構造は、文書上での表現実体となるコンテンツ情報である文書情報ファイルと、この文書情報ファイルを表現実体化させ

る動作プログラムである動作プログラムファイルの保存位置を示す位置情報と、前記動作プログラムファイルに関する暗号化された特徴量を保持する特徴量保持ファイルと、をカプセル化手段によってカプセル化した。

【００２０】

したがって、文書情報ファイルを表現実体化させる動作プログラムファイルの保存位置を示す位置情報が当該文書情報ファイルと一体にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに所定位置に保存されている動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【００２１】

請求項６記載の発明のカプセル化文書構造は、文書上での表現実体となるコンテンツ情報である文書情報ファイルと、この文書情報ファイルを表現実体化させる動作プログラムであり、特徴量が外部に保持されている動作プログラムファイルと、をカプセル化手段によってカプセル化した。

【００２２】

したがって、文書情報ファイルを表現実体化させる動作プログラムファイルが当該文書情報ファイルと一体にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、配布された動作プログラムファイルの特徴量を算出し、外部に保持されている動作プログラムファイルの特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【００２３】

請求項７記載の発明のカプセル化文書構造は、文書上での表現実体となるコン

テンツ情報である文書情報ファイルと、この文書情報ファイルを表現実体化させる動作プログラムであり、特徴量が外部に保持されている動作プログラムファイルの保存位置を示す位置情報と、をカプセル化手段によってカプセル化した。

【００２４】

したがって、文書情報ファイルを表現実体化させる動作プログラムファイルの保存位置を示す位置情報が当該文書情報のファイルと一体にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、所定位置に保存されている動作プログラムファイルの特徴量を算出し、外部に保持されている動作プログラムファイルの特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【００２５】

請求項８記載の発明は、請求項３ないし５の何れか一記載のカプセル化文書構造において、前記特徴量保持ファイルには、前記文書情報ファイルに関する暗号化された特徴量も保持されている。

【００２６】

したがって、動作プログラムファイルの改ざん検証のみならず、文書情報ファイルの改ざん検証が可能になるので、更に安全に文書を閲覧することが可能になる。

【００２７】

請求項９記載の発明は、請求項３ないし５の何れか一記載のカプセル化文書構造において、前記特徴量保持ファイルには、前記動作プログラムファイルに関する暗号化された特徴量に対応付けられて前記暗号化された特徴量を復号化する復号化鍵情報が保持されている。

【００２８】

したがって、復号化鍵情報をカプセル化文書ファイル内にカプセル化して閲覧者に配布することによって、閲覧者はカプセル化文書ファイルを取得するだけで動作プログラムファイル等の改ざん検証が可能となる。

【００２９】

請求項１０記載の発明は、請求項３ないし５の何れか一記載のカプセル化文書構造において、前記特徴量保持ファイルには、前記動作プログラムファイルに関する暗号化された特徴量に対応付けられて前記暗号化された特徴量を復号化する復号化鍵情報の保存位置を示す位置情報が保持されている。

【００３０】

したがって、復号化鍵情報の保存位置を示す位置情報をカプセル化文書ファイル内にカプセル化して閲覧者に配布することによって、閲覧者はカプセル化文書ファイルを取得するだけで動作プログラムファイル等の改ざん検証が可能となる。

【００３１】

請求項１１記載の発明は、請求項９または１０記載のカプセル化文書構造において、各動作プログラムファイル毎に異なる前記復号化鍵情報が対応付けられている。

【００３２】

したがって、例えば１つのベンダーだけでなく複数のベンダーによって複数の動作プログラムファイルが作成されるような場合、閲覧者は、各ベンダーの復号化鍵情報を使用することによって動作プログラムファイルの改ざん検証を行うことが可能になる。これにより、ベンダーごとに作成した動作プログラムファイルに対して、責任を持たせることが可能なカプセル化文書ファイルを提供することが可能になる。

【００３３】

請求項１２記載の発明は、請求項３ないし１１の何れか一記載のカプセル化文書構造において、前記動作プログラムファイルに関する特徴量は、公開鍵暗号方式により暗号化されている。

【００３４】

したがって、カプセル化文書ファイルの生成者が所有して公開しない秘密鍵を暗号化鍵とし、秘密鍵とは異なる公開鍵を復号化鍵として閲覧者に公開することにより、公開鍵を有する者だけが動作プログラムファイルに関する特徴量を復号

化することが可能になる。

【００３５】

請求項１３記載の発明は、請求項１２記載のカプセル化文書構造において、前記復号化鍵情報は、第三者認証局により署名暗号化されている。

【００３６】

したがって、第三者認証局が作成者側の復号化鍵情報（公開鍵情報）を署名し、カプセル化文書ファイルの信頼性を保証することにより、閲覧者が作成者を既知でなくとも作成者の危険性を判定してカプセル化文書ファイルのセキュリティ機能を保つことが可能になる。

【００３７】

請求項１４記載の発明は、請求項３ないし１１の何れか一記載のカプセル化文書構造において、前記動作プログラムファイルに関する特徴量は、秘密鍵暗号方式により暗号化されている。

【００３８】

したがって、暗号化鍵と復号化鍵とが同一の鍵であることにより、暗号化や復号化を高速に実行することが可能になる。

【００３９】

請求項１５記載の発明は、請求項３ないし１４の何れか一記載のカプセル化文書構造において、前記動作プログラムファイルの改ざん検証を実行する特徴量検証プログラムファイルをカプセル化手段によってカプセル化した。

【００４０】

したがって、カプセル化文書ファイル内に特徴量検証プログラムファイルを挿入し、起動プログラムが特徴量検証プログラムファイルの改ざん検証と特徴量検証プログラムの起動とを実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことが可能となる。

【００４１】

請求項１６記載の発明の記憶媒体は、請求項３ないし１５の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを格納した。

【００４２】

したがって、請求項３ないし１５の何れか一記載の発明と同様の作用を奏する。

【００４３】

請求項１７記載の発明のカプセル化文書作成装置は、文書上での表現実体となるコンテンツ情報である文書情報ファイルを取得する文書情報ファイル取得手段と、コンピュータにより解釈、実行されて、前記文書情報ファイル取得手段により取得された前記文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルを取得する動作プログラムファイル取得手段と、前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、この特徴量算出手段により算出した前記動作プログラムファイルの特徴量を暗号化鍵情報で暗号化し、特徴量保持ファイルに保存する特徴量保持ファイル生成手段と、前記文書情報ファイルと前記動作プログラムファイルと前記特徴量保持ファイルとを単一の文書としてカプセル化するカプセル化手段と、を備える。

【００４４】

したがって、セキュリティ性の高い請求項４記載のファイル構造のカプセル化文書ファイルを簡単に作成することが可能になる。

【００４５】

請求項１８記載の発明は、請求項１７記載のカプセル化文書作成装置において、前記文書情報ファイルの特徴量を算出する文書情報特徴量算出手段を備え、この文書情報特徴量算出手段により算出した前記文書情報ファイルの特徴量も暗号化鍵情報で暗号化し、前記特徴量保持ファイルに保存する。

【００４６】

したがって、セキュリティ性の高い請求項８記載のファイル構造のカプセル化文書ファイルを簡単に作成することが可能になる。

【００４７】

請求項１９記載の発明の改ざん検証装置は、請求項３ないし１５の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを読み込む読込み手段と、この読込み手段により読み込まれた前記カプセル化文書ファイルに保持された文書

情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、前記動作プログラムファイルの改ざん検証を実行する改ざん検証手段と、を備える。

【００４８】

したがって、カプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、動作プログラムファイルの改ざん検証が実行される。これにより、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【００４９】

請求項２０記載の発明は、請求項１９記載の改ざん検証装置において、前記改ざん検証手段は、前記読込み手段により読み込まれた前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量を復号化する復号化手段と、前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、この特徴量算出手段により算出された前記動作プログラムファイルの特徴量と前記復号化手段により復号化された前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、を備える。

【００５０】

したがって、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【００５１】

請求項２１記載の発明は、請求項１９記載の改ざん検証装置において、前記改ざん検証手段は、前記読込み手段により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、この特徴量算出手段により算出された前記動作プログラムファイルの特徴量

と起動プログラム内の前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、を備える。

【００５２】

したがって、配布された動作プログラムファイルの特徴量を算出し、起動プログラム内の特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【００５３】

請求項２２記載の発明は、請求項１９記載の改ざん検証装置において、前記改ざん検証手段は、前記読込み手段により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、この特徴量算出手段により算出された前記動作プログラムファイルの特徴量を暗号化する暗号化手段と、この暗号化手段により暗号化された前記動作プログラムファイルの暗号化特徴量と前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、を備える。

【００５４】

したがって、配布された動作プログラムファイルの特徴量を算出するとともに算出された動作プログラムファイルの特徴量を暗号化し、この暗号化した特徴量と特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【００５５】

請求項２３記載の発明は、請求項１９記載の改ざん検証装置において、前記改ざん検証手段は、前記読込み手段により読み込まれた前記カプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出する特徴量算出手段と、この特徴量算出手段により算出された前記特徴量検証プログラムファイル

の特徴量と起動プログラム内の前記特徴量検証プログラムファイルの特徴量とに基づいて前記特徴量検証プログラムファイルを実行するか否かを判定する判定手段と、この判定手段により前記特徴量検証プログラムファイルを実行すると判定された場合、前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、を備える。

【００５６】

したがって、配布されたカプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出し、起動プログラム内の特徴量検証プログラムファイル特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における特徴量検証プログラムファイルの改ざん検証が可能になり、改ざんがなされていない場合に特徴量検証プログラムの起動を実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことが可能となる。

【００５７】

請求項２４記載の発明のカプセル化文書作成処理プログラムは、コンピュータにインストールされ、文書上での表現実体となるコンテンツ情報である文書情報ファイルを取得する文書情報ファイル取得機能と、コンピュータにより解釈、実行されて、前記文書情報ファイル取得機能により取得された前記文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルを取得する動作プログラムファイル取得機能と、前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、この特徴量算出機能により算出した前記動作プログラムファイルの特徴量を暗号化鍵情報で暗号化し、特徴量保持ファイルに保存する特徴量保持ファイル生成機能と、前記文書情報ファイルと前記動作プログラムファイルと前記特徴量保持ファイルとを単一の文書としてカプセル化するカプセル化機能と、をコンピュータに実行させる。

【００５８】

したがって、セキュリティ性の高い請求項４記載のファイル構造のカプセル化文書ファイルを簡単に作成することが可能になる。

【００５９】

請求項２５記載の発明は、請求項２４記載のカプセル化文書作成処理プログラムにおいて、前記文書情報ファイルの特徴量を算出する文書情報特徴量算出機能をコンピュータに実行させ、この文書情報特徴量算出機能により算出した前記文書情報ファイルの特徴量も暗号化鍵情報で暗号化し、前記特徴量保持ファイルに保存する。

【００６０】

したがって、セキュリティ性の高い請求項８記載のファイル構造のカプセル化文書ファイルを簡単に作成することが可能になる。

【００６１】

請求項２６記載の発明の記憶媒体は、請求項２４または２５記載のカプセル化文書作成処理プログラムを記憶する。

【００６２】

したがって、この記憶媒体に記憶されたカプセル化文書作成処理プログラムをコンピュータに読み取らせることにより、セキュリティ性の高い請求項４または８記載のファイル構造のカプセル化文書ファイルを簡単に作成することが可能になる。

【００６３】

請求項２７記載の発明の起動プログラムは、請求項３ないし１５の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを読み込む読込み機能と、この読込み機能により読み込まれた前記カプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、前記動作プログラムファイルの改ざん検証を実行する改ざん検証機能と、をコンピュータに実行させる。

【００６４】

したがって、カプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、動作プログラムファイルの改ざん検証が実行される。これにより、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【００６５】

請求項２８記載の発明は、請求項２７記載の起動プログラムにおいて、前記改ざん検証機能は、前記読込み機能により読み込まれた前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量を復号化する復号化機能と、前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、この特徴量算出機能により算出された前記動作プログラムファイルの特徴量と前記復号化機能により復号化された前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、をコンピュータに実行させる。

【００６６】

したがって、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【００６７】

請求項２９記載の発明は、請求項２７記載の起動プログラムにおいて、前記改ざん検証機能は、前記読込み機能により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、この特徴量算出機能により算出された前記動作プログラムファイルの特徴量と起動プログラム内の前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、をコンピュータに実行させる。

【００６８】

したがって、配布された動作プログラムファイルの特徴量を算出し、起動プログラム内の特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【００６９】

請求項３０記載の発明は、請求項２７記載の起動プログラムにおいて、前記改ざん検証機能は、前記読込み機能により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、この特徴量算出機能により算出された前記動作プログラムファイルの特徴量を暗号化する暗号化機能と、この暗号化機能により暗号化された前記動作プログラムファイルの暗号化特徴量と前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、をコンピュータに実行させる。

【００７０】

したがって、配布された動作プログラムファイルの特徴量を算出するとともに算出された動作プログラムファイルの特徴量を暗号化し、この暗号化した特徴量と特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【００７１】

請求項３１記載の発明は、請求項２７記載の起動プログラムにおいて、前記改ざん検証機能は、前記読込み機能により読み込まれた前記カプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出する特徴量算出機能と、この特徴量算出機能により算出された前記特徴量検証プログラムファイルの特徴量と起動プログラム内の前記特徴量検証プログラムファイルの特徴量とに基づいて前記特徴量検証プログラムファイルを実行するか否かを判定する判定機能と、この判定機能により前記特徴量検証プログラムファイルを実行すると判定された場合、前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、をコンピュータに実行させる。

【００７２】

したがって、配布されたカプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出し、起動プログラム内の特徴量検証プログラムフ

ァイル特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における特徴量検証プログラムファイルの改ざん検証が可能になり、改ざんがなされていない場合に特徴量検証プログラムの起動を実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことが可能となる。

【００７３】

請求項３２記載の発明の記憶媒体は、請求項２７ないし３１のいずれか一記載の起動プログラムを記憶する。

【００７４】

したがって、この記憶媒体に記憶されたカプセル化文書作成処理プログラムをコンピュータに読み取らせることにより、請求項２７ないし３１のいずれか一記載の発明と同様の作用を奏する。

【００７５】

【発明の実施の形態】

[第一の実施の形態]

本発明の第一の実施の形態を図１ないし図８に基づいて説明する。

【００７６】

本発明は、パーソナルコンピュータに代表される各種情報処理装置によって動作する文書のデータ構造（カプセル化文書構造）とその実装形態に関するものであるので、まず、一般的なパーソナルコンピュータで説明する。

【００７７】

[１．パーソナルコンピュータ１の構成についての説明]

図１は本実施の形態も適用される一般的又は標準的なパーソナルコンピュータ１のハードウェアの構成図である。パーソナルコンピュータ（以下、コンピュータと略す。）１は、情報処理を行う情報処理部であるＣＰＵ（Central Processing Unit）２と、ＢＩＯＳ（Basic Input Output System）等を格納するＲＯＭ（Read Only Memory）３と、情報を処理中に一時的に格納するＲＡＭ（Random Access Memory）４等の一次記憶装置と、アプリケーションプログラムや処理結果等を保存するＨＤＤ（Hard Disk Drive）５等の二次記憶装置と、情報を外部に保

管又は配布し若しくは情報（カプセル化文書ファイル２１（図３参照）やアプリケーションプログラム）を外部から入手するための記憶媒体であるリムーバブルメディア６のドライブ６ａと、外部の他のコンピュータ１′，…と通信するためのネットワーク７に接続するためのネットワークインタフェース８と、処理経過や処理結果等をユーザに表示するディスプレイ９と、操作者がコンピュータ１に命令や情報等を入力するためのキーボード１０やマウス１１等の入力装置とから構成され、これらの間のデータ通信をバスコントローラ１２が調停して動作している。

【００７８】

なお、リムーバブルメディア６としては、フレキシブルディスク、ハードディスク、磁気テープ等のような磁気的な記憶媒体、ＭＯのような光磁気的な記憶媒体、ＣＤ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ－ＲＯＭ、ＤＶＤ－Ｒ、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＷ、ＤＶＤ＋ＲＷ等のような光学的な記憶媒体、半導体メモリ等、各種の記憶媒体が適用できる。

【００７９】

データ送信は、コンピュータ１のネットワークインタフェース８へとデータを送ることにより、ネットワークインタフェース８がネットワーク７へと信号を出力する。また、ネットワークインタフェース８が受け取った信号については、ネットワークインタフェース８において必要かどうかの判断がなされ、必要なデータであれば取り込み、不必要であれば破棄する、というような処理が行われる。すなわち、あらゆるデータの送受信は、すべてネットワークインタフェース８を経由して行われることになる。

【００８０】

一般的に、このようなコンピュータ１ではユーザが電源を投入すると、ＣＰＵ２はＲＯＭ３内のＢＩＯＳに含まれるローダーというプログラムを起動させ、ＨＤＤ５からオペレーティングシステム（ＯＳ）という当該コンピュータ１のハードウェアとソフトウェアとを管理するプログラムをＲＡＭ４に読み込む。ＯＳは起動すると、ユーザの操作に応じてアプリケーションプログラムの起動、情報の読み込み、保存等をサポートする。代表的なＯＳとしては、Windows（Microso

ft Corporationの登録商標）、ＵＮＩＸ（X/Open, Inc.の登録商標）等が知られている。これらのＯＳ上で走るプログラムをアプリケーションプログラムと呼んでいる。ユーザは、通常、このＯＳを通してユーザの目的とするアプリケーションプログラムを起動、必要なデータを編集、保存、消去等を行うために記憶装置に記録されているデジタル情報をファイルと言う単位で操作する。つまり、ユーザがコンピュータに対して各種の操作を行う場合はアプリケーションプログラムやデータは全て“ファイル”と言う単位で扱い、それらは記憶装置に保持されている。

【００８１】

次に、ＯＳが二次記憶装置等の記憶媒体に保持されているアプリケーションプログラムをユーザの指示により起動する場合について図２を参照して説明する。ユーザがＯＳに特定のプログラムの起動を指示すると、ＯＳはそのプログラムコードを記憶媒体より記憶装置のハードウェアを使用して読み込み、これをコンピュータ１の一次記憶装置（メモリ）であるＲＡＭ４にコードを展開し、展開された特定のアドレスよりＣＰＵ２が実行することでプログラムが実行される。通常、このような独立に実行されているプログラムのことを“プロセス”又は“タスク”と称し、記憶媒体に保持された“プログラムコード”と区別している。

【００８２】

現在の多くのＯＳは、このようなプロセス又はタスクを複数同時に走らせることのできるマルチタスク機能を有するものが一般的である。また、今日のＯＳはこのような複数のプロセスを同時に走らせるためにプロセス毎に独立してメモリを割り当て動作している。

【００８３】

また、このようなプロセス間でデータをやり取りするプロセス間通信のためにメモリ上にメタファイルと言う仮想的なファイルを形成し、ファイルアクセスを介して情報の送受信を行っている。

【００８４】

［２．カプセル化文書の説明］

次に、本発明の特長の１つである文書のデータ構造（カプセル化文書構造）の

概要について図３を参照して説明する。このカプセル化文書ファイル２１は、コンピュータ１のＨＤＤ５に保持されている。本実施の形態のカプセル化文書ファイル２１は、文書上での表現実体となる各種のコンテンツや文書構造をファイル化した文書情報ファイル２２と、文書情報ファイル２２のコンテンツを表現実体化（表示、動作、閲覧等）させる動作プログラムの動作プログラムファイル２３と、特徴量保持ファイル２４とを、単一の文書としてカプセル化手段を用いてカプセル化したものである。これらの情報は、各々一般的なコンピュータ１のＯＳが管理できる個別のファイル単位の構造となっている。

【００８５】

より詳細には、文書情報ファイル２２のコンテンツ情報は、静止画像、動画像、音声、テキストファイル等であってコンピュータ１で使用、動作出来るファイルフォーマットに準じてファイル化されている。また、カプセル化手段には、ＺＩＰ、ＬＨＡ等の周知のマルチファイル圧縮方式を使用し、各文書情報ファイル２２を閲覧等で表示する場合はこれらのマルチファイル圧縮フォーマットで符号化されているファイルを動的に復号化することで使用する。また、動作プログラムファイル２３の動作プログラムは、中間言語コードで記述されている事が望ましい。動作プログラムが中間言語で記述されていれば、この中間言語を解釈実行できるコンパイラまたはインタプリタプログラムがコンピュータにインストールされている状況においてコンピュータの機種依存性が無くなる。このような中間言語としては、java（Sun Microsystemsの登録商標）言語がある。

【００８６】

さらに、図３に示すように、特徴量保持ファイル２４には、各動作プログラムファイル２３の特徴量を暗号化したものが保存されている。

【００８７】

すなわち、従来の技術と異なる点は、各動作プログラムファイル２３の特徴量が暗号化されて保存されている特徴量保持ファイル２４をカプセル化文書ファイル２１に保持している点である。

【００８８】

したがって、文書情報ファイル２２を表現実体化させる動作プログラムファイ

ル２３が当該文書情報ファイル２２と一体にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、特徴量保持ファイル２４に保持されている動作プログラムファイル２３の暗号化特徴量を復号化するとともに配布された動作プログラムファイル２３の特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイル２１の配布途中における動作プログラムファイル２３の改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【００８９】

［３．コンピュータ１が備える特長的な機能の説明］

次に、コンピュータ１が備える特長的な機能について説明する。

【００９０】

［３－１．カプセル化文書作成処理］

コンピュータ１は、内蔵するＣＰＵ２がＯＳ上で動作するアプリケーションプログラムに従うことにより、カプセル化文書ファイル２１を作成するカプセル化文書作成処理を実行するカプセル化文書作成装置として機能することになる。図４は、ＣＰＵ２がＯＳ上で動作するアプリケーションプログラムに従うことにより実現されるカプセル化文書作成処理の流れを示すフローチャートである。

【００９１】

図４に示すように、まず、ユーザの操作に応じて文書上での表現実体となるコンテンツ（閲覧者へ伝えたい文書内容）である文書情報ファイル２２を生成する（ステップＳ１：文書情報ファイル取得手段）。このような文書情報ファイル２２の生成は、一般のワードプロセッシングソフト等により実現可能である。次いで、文書情報ファイル２２内のコンテンツを表現実体化（表示、動作、閲覧等）させる動作プログラムファイル２３を生成する（ステップＳ２：動作プログラムファイル取得手段）。

【００９２】

続くステップＳ３においては、ステップＳ２で生成した動作プログラムファイル２３の特徴量を算出する。ここに、特徴量算出手段の機能が実行される。動作

プログラムファイル２３の特徴量とは、動作プログラムファイル２３に対する電子指紋である。このような特徴量の算出方法としては、ＳＨＡ１（Secure-Hash-Algorithm）などが挙げられる。ＳＨＡ１では、動作プログラムとなる任意の長さのデータブロックを２０バイトのシーケンスで圧縮する。実際の指紋と同様に２つの異なる動作プログラムの特徴量は、必ず異なることを期待されるが、特徴量の値の種類は有限であるために異なる動作プログラムにおいても同じ特徴量が算出される可能性がある。しかし、特徴量は２１６０種類という莫大な数へと変換できるため、異なる動作プログラムから同一の特徴量を生成する可能性を確率的に無視することができる。ＳＨＡ１の基本的な特性として、動作プログラムを１ビットでも変更すると動作プログラムの特徴量も変更されることと、特徴量の偽造を試みても元の特徴量と同じ特徴量を持つ偽造メッセージを生成できないことの２点が挙げられる。この特性により、動作プログラムと動作プログラムの特徴量が一対一の関係となることが立証される。ＳＨＡ１以外の特徴量の算出方法としては、Massachusetts Institute of TechnologyのRonald Rivest氏が発明したＭＤ５なども挙げられる。なお、動作プログラムファイル２３の特徴量の算出には、ＳＨＡ１、ＭＤ５以外の手法を使用しても良い。また、特徴量算出の実行手段の一例としては、動作プログラムがjava言語で記載されているときには、Sun Microsystems社から提供されているjavaのsecurityパッケージにあるプログラムを使用することによって容易に特徴量を算出できる。

【００９３】

次いで、秘密鍵・公開鍵を生成し（ステップＳ４）、生成した秘密鍵で動作プログラムファイル２３の特徴量を暗号化する（ステップＳ５）。秘密鍵を利用した暗号化には、ＲＳＡやＤＳＡ（Digital Signature Algorithm）などを利用する。ＲＳＡの暗号アルゴリズムは大きな数値の素因数分解を実行することが困難であるという事実に依存したものであり、2000ビット以上の係数を持つ鍵であれば安全であると一般的に知られている。ＲＳＡ、ＤＳＡなどは、様々な企業から提供されているため、簡単に使用することが可能である。なお、暗号化に使用する秘密鍵・公開鍵を生成する代わりに、作成者のコンピュータ内に予め保持された秘密鍵・公開鍵を使用するようにしても良い。

【００９４】

すなわち、本実施の形態においては、公開鍵暗号方式により動作プログラムファイル２３の特徴量を暗号化するものである。これにより、カプセル化文書ファイル２１の生成者が所有して公開しない秘密鍵を暗号化鍵とし、秘密鍵とは異なる公開鍵を復号化鍵として閲覧者に公開することにより、公開鍵を有する者だけが動作プログラムファイル２３に関する特徴量を復号化することが可能になる。

【００９５】

そして、このように秘密鍵で暗号化された動作プログラムファイル２３の特徴量を特徴量保持ファイル２４に保存した後（ステップＳ６：特徴量保持ファイル生成手段）、文書情報ファイル２２と動作プログラムファイル２３と特徴量保持ファイル２４とを単一の文書としてカプセル化手段を用いてカプセル化したカプセル化文書ファイル２１を作成する（ステップＳ７）。なお、暗号化された動作プログラムファイル２３の特徴量を特徴量保持ファイル２４に保存する際には、動作プログラムファイル２３と暗号化された動作プログラムファイルの特徴量との対応が付くようにしておく。暗号化された動作プログラムファイル２３の特徴量を動作プログラムファイル２３に対応付けてＸＭＬで表記した例を図５に示す。図５に示すように、特徴量保持ファイル２４には、動作プログラムタグ内の属性情報として、暗号化された動作プログラムファイルの特徴量が保存されている。また、図５に示すように、特徴量保持ファイル２４の特徴量算出情報タグ内の属性情報であるアルゴリズムには、作成者が動作プログラムファイル２３の特徴量を算出した際に使用した特徴量算出アルゴリズムが記載されている。

【００９６】

以上のようにして作成されたカプセル化文書ファイル２１は、動作プログラムファイル２３の特徴量の暗号化に使用された秘密鍵と対になる公開鍵とともに、ネットワーク７を介して所定のコンピュータ１に対して送信されて配布されることになる。

【００９７】

［３－２．改ざん検証処理］

コンピュータ１は、内蔵するＣＰＵ２がＯＳ内にあるShellプログラムが関連

付けされているカプセル化文書起動プログラム（以下、起動プログラムという。）に従うことにより、動作プログラムファイル２３の改ざん検証処理を実行する改ざん検証装置として機能することになる。ここでは、図３に示すようなカプセル化文書ファイル２１が公開鍵とともに別のコンピュータ１（カプセル化文書作成装置）から配布されたものとして説明する。

【００９８】

閲覧者がキーボード１０やマウス１１等の入力装置を介してカプセル化文書ファイル２１を選択した際に、ＯＳ内にあるShellプログラムが拡張子等でカプセル化文書ファイル２１と判断した場合には、起動プログラムが起動する。起動プログラムは、選択されたカプセル化文書ファイル２１を読み込み、カプセル化文書ファイル２１内にある動作プログラムファイル２３の改ざん検証をする。

【００９９】

図６は、起動プログラムによる改ざん検証処理の流れを示すフローチャートである。図６に示すように、まず、配布されたカプセル化文書ファイル２１と公開鍵を取得して解凍すると（ステップＳ１１：読込み手段）、取得した公開鍵を使用してカプセル化文書ファイル２１内にある暗号化された動作プログラムファイル２３の特徴量を復号化する（ステップＳ１２：復号化手段）。

【０１００】

次いで、ステップＳ１１で取得したカプセル化文書ファイル２１内の動作プログラムファイル２３の特徴量を算出する（ステップＳ１３：特徴量算出手段）。動作プログラムファイル２３の特徴量の算出は、カプセル化文書作成装置での処理と同様に、ＳＨＡ１、ＭＤ５の手法を使用しても良いし、javaのsecurityパッケージにあるプログラムを使用しても良いが、原則的には作成者側と閲覧者側との特徴量算出アルゴリズムを一致させることが必要である。前述したように、特徴量保持ファイル２４の特徴量算出情報タグ内の属性情報であるアルゴリズムには、作成者が動作プログラムファイル２３の特徴量を算出した際に使用した特徴量算出アルゴリズムが記載されているので（図５参照）、この特徴量算出アルゴリズム情報に基づいて動作プログラムファイル２３の特徴量の算出を行えば良い。なお、作成者側と閲覧者側との特徴量算出アルゴリズムが対応していれば、必

ずしも同一の特徴量算出アルゴリズムで動作プログラムファイル２３の特徴量を算出しなくても良い。

【０１０１】

次いで、ステップＳ１４に進み、配布されたカプセル化文書ファイル２１内の暗号化された動作プログラムファイル２３の特徴量を復号化した値と閲覧者側で動作プログラムファイル２３の特徴量を算出した値とを比較し、動作プログラムファイル２３の改ざん検証を実行する。ここに、改ざん検証実行手段の機能が実行される。ここで、同一の特徴量算出アルゴリズムを使用して同一な動作プログラムファイル２３の特徴量を算出することにより、カプセル化文書ファイル２１内の動作プログラムファイル２３に改ざんがなければ、配布されたカプセル化文書ファイル２１内の暗号化された動作プログラムファイル２３の特徴量を復号化した値と閲覧者側で動作プログラムファイル２３の特徴量を算出した値は一致することになる。したがって、２つの特徴量を比較することにより、動作プログラムファイル２３の改ざんを検証することができる。

【０１０２】

つまり、ステップＳ１２～Ｓ１４において、改ざん検証手段の機能が実行される。

【０１０３】

動作プログラムファイル２３の改ざん検証を行った結果、２つの特徴量が一致していれば、すなわち動作プログラムファイル２３が改ざんされていなければ（ステップＳ１５のＮ）、動作プログラムファイル２３に記載された署名情報をディスプレイ９に表示し（ステップＳ１６）、表示された署名者が信用できるかを閲覧者に判断させる。

【０１０４】

信用できる署名者である旨がキーボード１０やマウス１１等の入力装置を介して閲覧者により入力された場合には（ステップＳ１７のＹ）、動作プログラムファイル２３の動作プログラムを実行してディスプレイ９上にカプセル化文書ファイル２１内の文書情報ファイル２２を表示する（ステップＳ１８）。

【０１０５】

一方、動作プログラムファイル２３の改ざん検証を行った結果、２つの特徴量が一致しなければ、すなわち動作プログラムファイル２３が改ざんされている場合（ステップＳ１５のＹ）、信用できる署名者でない旨がキーボード１０やマウス１１等の入力装置を介して閲覧者により入力された場合には（ステップＳ１７のＮ）、動作プログラムファイル２３の動作プログラムを実行せずに、不正なプログラムファイルであることを報知する不正報知処理を実行する（ステップＳ１９）。不正報知処理としては、例えば、カプセル化文書ファイル２１内の動作プログラムファイル２３が配布途中で改ざんされたことを通知するダイアログボックスをディスプレイ９上に表示することが考えられる。また、不正なプログラムファイルである旨を表示するのみに留まらず、カプセル化文書ファイル２１の動作プログラムファイル２３を消去するかどうかユーザに促しても良い。

【０１０６】

通常、特徴量情報は２０バイトの情報量で生成されるが、改ざん検証を行う動作プログラムファイル２３の危険性に応じて、特徴量情報の情報量を変化させても良い。動作プログラムファイル２３の改ざん検証を行う際に使用する動作プログラムファイル２３の特徴量情報の情報量は、小さい方が高速に動作プログラムファイル２３の改ざん検証を実行できるが、あまりにも小さすぎると特徴量のバリエーションが乏しくなり改ざんされる危険性が増加する。したがって、危険性の低い動作プログラムファイル２３は小さな情報量となるように特徴量情報を算出し、危険性の高い動作プログラムファイル２３は大きな情報量となるように特徴量情報を算出しても良い。この際、閲覧者側へ動作プログラムファイル２３の改ざん検証がどれだけ安全に機能しているかを通知するために、改ざん検証に使用された特徴量情報の情報量の大きさを閲覧者側へ表示させる必要がある。そこで、特徴量保持ファイル２４内に保持される暗号化された動作プログラムファイル２３の特徴量を復号化した値又は閲覧者側で動作プログラムファイル２３の特徴量を算出した値を、ディスプレイ９上に表示するようにしても良い。このように特徴量情報を閲覧者側のコンピュータ１のディスプレイ９へ表示するための特徴量情報表示プログラムファイルをカプセル化文書ファイル２１内にカプセル化することによって、閲覧者側へ改ざん検証機能の安全性を通知することのできる

カプセル化文書ファイルを提供することができる。

【０１０７】

このように本実施の形態によれば、カプセル化文書作成装置と改ざん検証装置とを備え、動作プログラムファイル２３全体を暗号化処理せずとも、動作プログラムファイル２３の特徴量という２０バイト程度の小さなデータを暗号化処理するだけで、カプセル化文書ファイル２１の配布途中における動作プログラムファイル２３の改ざん検証ができる。これにより、高速にカプセル化文書ファイル２１内の動作プログラムファイル２３の改ざん検証が実行できる利便性の高いカプセル化文書ファイル２１を提供することができる。

【０１０８】

なお、起動プログラムは、ＯＳ内にあるShellプログラムで起動するものに限るものではなく、Shellプログラムがこの様な機能を有しても良い。

【０１０９】

なお、動作プログラムファイル２３を暗号化する秘密鍵を複数用意し、動作プログラムファイル２３の動作権限に対応させて復号化する公開鍵を変更するようにしても良い。動作プログラムの実行内容によって動作プログラムファイル２３の危険性は変化することが考えられる。例えば、動作プログラムファイル２３が文書情報ファイル２２を表示するだけならば危険性は少ないが、動作プログラムファイル２３が文書情報ファイル２２を編集する機能を追加する場合には動作プログラムファイル２３の危険性が高くなる。そこで、閲覧者側のコンピュータ１には予め動作プログラムファイル２３の処理を制限する動作制限情報を設定しておき、動作制限情報に対応させて復号化する公開鍵を変更することにより、危険性の高い動作プログラムファイル２３を実行させないようにすることが可能になる。

【０１１０】

より具体的には、図７に示すように、ファイルの読み書き、ネットワークの送受信等を許可（○で示す）、非許可（×で示す）の動作権限のモードに応じて復号化する公開鍵を用意し、動作プログラムファイル２３を実行する際に必要な公開鍵の動作権限情報をディスプレイ９を通じて閲覧者に表示することで、閲覧者

に許可をもらってそのモードの動作権限で動作プログラムファイル２３を起動しても良い。例えば図７に示す動作権限モードがＢであれば、カプセル化文書ファイル２１内のファイルを読み込むプログラムだけを実行させる。同様にして動作権限モードがＣであれば、カプセル化文書ファイル２１内のファイルを読込むプログラム及びコンピュータ１内のファイルを読込むプログラムだけが実行される。

【０１１１】

動作プログラムの動作権限を制限する方法は、上述した方法に限るものではない。例えば、動作プログラムに中間コードを使用する場合はこれを解釈実行するのにインタプリタが必要になりこのインタプリタを通してコンピュータの入出力を行うので簡単に動作権限を制限できる。また、動作プログラムがネイティブなコードの場合は実行に先立って実行コードを検出し、権限外の動作を制限すれば良い。また、このような動作権限の制限機能は現在の標準的なオペレーティングシステムに備わっているのでこれを利用しても良い。

【０１１２】

以上により、閲覧者側の動作制限情報に応じて動作プログラムファイル２３を実行するカプセル化文書ファイル２１が提供できる。

【０１１３】

また、動作プログラムファイル２３の１つとして動作権限情報通知プログラムを追加し、閲覧者側の動作権限情報を作成者へ知らせるようにしても良い。動作権限情報通知プログラムは、閲覧者側のコンピュータ１のディスプレイ９上に動作権限情報を作成者へ通知しても良いかを判定させるダイアログボックスを表示させる。閲覧者が動作権限情報の通知を許諾すれば、動作権限情報通知プログラムを実行して閲覧者側のコンピュータ１内に設定されている動作権限情報を作成者側へ通知する。作成者は、閲覧者側から通知された動作権限情報を見て、閲覧者側の動作権限情報によって以前に配布したカプセル化文書ファイル２１内にある文書情報ファイル２２が表示されないと判断したときには、閲覧者側の動作権限情報に応じて動作プログラムファイル２３を変更したカプセル化文書ファイル２１を再度、閲覧者へ配布しても良い。

【０１１４】

これにより、動作プログラムファイル２３の閲覧者側の動作権限情報によって制限されるときには、作成者へカプセル化文書ファイル２１内の動作プログラムファイル２３が閲覧者側で起動されないことを通知するカプセル化文書ファイル２１を提供することができる。

【０１１５】

なお、本実施の形態においては、暗号化された動作プログラムファイル２３の特徴量を復号化したものと閲覧者側で動作プログラムファイル２３の特徴量を算出したものとを比較し、動作プログラムファイル２３の改ざん検証を実行するようにしたが、これに限るものではなく、暗号化された動作プログラムファイル２３の特徴量と閲覧者側で算出した動作プログラムファイル２３の特徴量を暗号化したもの（暗号化手段）とを比較し、動作プログラムファイル２３の改ざん検証を実行するようにしても良い。

【０１１６】

［４．本実施の形態の変形例］

［４－１．第１の変形例］

本実施の形態においてはカプセル化文書ファイル２１を公開鍵とともに配布するようにしたが、公開鍵をカプセル化文書ファイル２１内にカプセル化するようにしても良い。秘密鍵により暗号化された動作プログラムファイル２３の特徴量と、この秘密鍵と対になる公開鍵の情報である公開鍵情報とを動作プログラムファイル２３に対応付けてＸＭＬで表記した例を図８に示す。図８に示すように、特徴量保持ファイル２４には、動作プログラムタグ内の属性情報として、秘密鍵により暗号化された動作プログラムファイル２３の特徴量と、この秘密鍵と対になる公開鍵の情報である公開鍵情報とが保存されている。

【０１１７】

ところで、特徴量保持ファイル２４の公開鍵情報としては、公開鍵そのものに限るものではなく、公開鍵の位置情報であっても良い。例えば、公開鍵が保持されているインターネット上の位置情報（ＵＲＬ（Uniform Resource Locator））を記述しても良い（図８に示す“動作プログラム３”の公開鍵情報）。この場合

は、インターネットにコンピュータ１が接続されていることが前提になる。また、インターネット上に公開された公開鍵情報は、閲覧者が接続した際に閲覧者のコンピュータ１の記憶媒体（ＲＡＭ４やＨＤＤ５等）へ保存されるようにしても良い。このようにすることで、カプセル化文書ファイル２１内に公開鍵情報が保存されていない場合は、閲覧者のコンピュータの記憶媒体（ＲＡＭ４やＨＤＤ５等）に保存された公開鍵情報を代わりに使用することができる。

【０１１８】

このように公開鍵（公開鍵の位置情報）をカプセル化文書ファイル２１内にカプセル化して閲覧者に配布することによって、閲覧者は改ざん検証装置を用いてカプセル化文書ファイル２１を取得するだけで動作プログラムファイル２３の改ざん検証が可能となる。

【０１１９】

このような第１の変形例の具体例としては、各ベンダーが作成した動作プログラムファイル２３の特徴量に対して秘密鍵により暗号化を行い、復号化するための公開鍵情報を特徴量保持ファイル２４に保存するような場合が考えられる。図８に示すように、例えば動作プログラム１はベンダーＡ社で、動作プログラム２はベンダーＢ社で作成するような場合である。このような事態が生じるのは、現在のプログラム開発は、一人で全プログラムを作成する例は少なく、多人数で協力し合いながらプログラムを作成することが一般的であり、大規模なプログラムとなると１つのベンダーだけでなく複数のベンダーによって複数の動作プログラムファイルが作成されるためである。つまり、カプセル化文書ファイル２１内にカプセル化される動作プログラムファイル２３も、複数のベンダーによって作成されることが予想される。

【０１２０】

閲覧者は、特徴量保持ファイル２４に保存されている各ベンダーの公開鍵情報を使用することによって動作プログラムファイル２３の改ざん検証を行い、検証の際、動作プログラムファイル２３の改ざんがなければ、動作プログラムファイル２３を作成したベンダーの署名情報を表示し、動作プログラムファイル２３を実行する。

【０１２１】

このように各動作プログラムファイル２３毎に異なる公開鍵情報が対応付けられることにより、ベンダーごとに作成した動作プログラムファイル２３に対して、責任を持たせることが可能なカプセル化文書ファイル２１を提供することができる。

【０１２２】

［４－２．第２の変形例］

本実施の形態においては、文書情報ファイル２２と動作プログラムファイル２３と特徴量保持ファイル２４とを単一の文書としてカプセル化手段を用いてカプセル化したカプセル化文書ファイル２１を配布するようにしたが、カプセル化文書ファイル２１内に動作プログラムファイル２３を必ずしも保持しなくとも良い。このような場合、特徴量保持ファイル２４において“動作プログラムファイルと暗号化された動作プログラムファイルの特徴量”の対応が付けられるように位置情報を追加するなどの工夫が必要となる。位置情報を追加して動作プログラムの特徴量情報を保存した特徴量保持ファイル２４のファイルフォーマット例を図９に示す。図９に示すように、動作プログラムタグ内の属性情報として記載された位置情報としては、動作プログラムが保存されているインターネット上の位置情報（ＵＲＬ（Uniform Resource Locator））を記述しても良い。この場合は、インターネットにコンピュータ１が接続されていることが前提になる。図９の特徴量には、動作プログラムタグ内の属性情報として記載された位置情報に位置する動作プログラムファイルの特徴量を作成者の秘密鍵で暗号化した結果が記載されている。図９に示すようなファイルフォーマットにすることによって、動作プログラムファイルが物理的に単一ファイルにカプセル化されていなくとも、動作プログラムファイル２３の改ざん検証が可能となる。

【０１２３】

したがって、文書情報ファイル２２を表現実体化させる動作プログラムファイル２３の保存位置を示す位置情報が当該文書情報ファイル２２と一体にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、特徴量保持ファイル２４に保持されている動作プロ

グラムファイル２３の暗号化特徴量を復号化するとともに所定位置に保存されている動作プログラムファイル２３の特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイル２１の配布途中における動作プログラムファイル２３の改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【０１２４】

なお、動作プログラムファイルの一部のみを動作プログラムファイル２３として文書情報ファイル２２や特徴量保持ファイル２４とともにカプセル化し、残りの動作プログラムファイルをインターネット上の所定の位置に保存するようにしても良い。

【０１２５】

[第二の実施の形態]

本発明の第二の実施の形態を図１０ないし図１２に基づいて説明する。なお、本発明の第一の実施の形態において説明した部分と同一部分については同一符号を用い、説明も省略する。

【０１２６】

[１．カプセル化文書の説明]

本発明の特長の１つである文書のデータ構造（カプセル化文書構造）の概要について図１０を参照して説明する。このカプセル化文書ファイル２１は、コンピュータ１のＨＤＤ５に保持されている。本実施の形態のカプセル化文書ファイル２１は、文書上での表現実体となる各種のコンテンツや文書構造をファイル化した文書情報ファイル２２と、文書情報ファイル２２を表現実体化させる動作プログラムの動作プログラムファイル２３と、特徴量保持ファイル２４とを、単一の文書としてカプセル化手段を用いてカプセル化したものである。これらの情報は、各々一般的なコンピュータ１のＯＳが管理できる個別のファイル単位の構造となっている。

【０１２７】

より詳細には、文書情報ファイル２２のコンテンツ情報は、静止画像、動画像、音声、テキストファイル等であってコンピュータ１で使用、動作出来るファイ

ルフォーマットに準じてファイル化されている。また、カプセル化手段には、ＺＩＰ、ＬＨＡ等の周知のマルチファイル圧縮方式を使用し、各文書情報ファイル２２を閲覧等で表示する場合はこれらのマルチファイル圧縮フォーマットで符号化されているファイルを動的に復号化することで使用する。また、動作プログラムファイル２３の動作プログラムは、中間言語コードで記述されている事が望ましい。動作プログラムが中間言語で記述されていれば、この中間言語を解釈実行できるコンパイラまたはインタプリタプログラムがコンピュータにインストールされている状況においてコンピュータの機種依存性が無くなる。このような中間言語としては、java（Sun Microsystemsの登録商標）言語がある。

【０１２８】

さらに、図１０に示すように、特徴量保持ファイル２４には、各動作プログラムファイル２３の特徴量を暗号化したものと、各文書情報ファイル２２の特徴量を暗号化したものとが保存されている。

【０１２９】

すなわち、従来の技術と異なる点は、各動作プログラムファイル２３の特徴量と各文書情報ファイル２２の特徴量とが暗号化されて保存されている特徴量保持ファイル２４をカプセル化文書ファイル２１に保持している点である。

【０１３０】

［２．コンピュータ１が備える特長的な機能の説明］

次に、コンピュータ１が備える特長的な機能について説明する。

【０１３１】

［２－１．カプセル化文書作成処理］

コンピュータ１は、内蔵するＣＰＵ２がＯＳ上で動作するアプリケーションプログラムに従うことにより、カプセル化文書ファイル２１を作成するカプセル化文書作成処理を実行するカプセル化文書作成装置として機能することになる。図１１は、ＣＰＵ２がＯＳ上で動作するアプリケーションプログラムに従うことにより実現されるカプセル化文書作成処理の流れを示すフローチャートである。

【０１３２】

図１１に示すように、まず、ユーザの操作に応じて文書上での表現実体となる

コンテンツ（閲覧者へ伝えたい文書内容）である文書情報ファイル２２を生成する（ステップＳ２１：文書情報ファイル取得手段）。このような文書情報ファイル２２の生成は、一般のワードプロセッシングソフト等により実現可能である。次いで、文書情報ファイル２２内のコンテンツを表現実体化（表示、動作、閲覧等）させる動作プログラムファイル２３を生成する（ステップＳ２２：動作プログラムファイル取得手段）。

【０１３３】

続くステップＳ２３においては、ステップＳ２２で生成した動作プログラムファイル２３の特徴量を算出する。ここに、特徴量算出手段の機能が実行される。動作プログラムファイル２３の特徴量とは、動作プログラムファイル２３に対する電子指紋である。このような特徴量の算出方法としては、ＳＨＡ１（Secure-Hash-Algorithm）などが挙げられる。ＳＨＡ１では、動作プログラムとなる任意の長さのデータブロックを２０バイトのシーケンスで圧縮する。実際の指紋と同様に２つの異なる動作プログラムの特徴量は、必ず異なることを期待されるが、特徴量の値の種類は有限であるために異なる動作プログラムにおいても同じ特徴量が算出される可能性がある。しかし、特徴量は２１６０種類という莫大な数へと変換できるため、異なる動作プログラムから同一の特徴量を生成する可能性を確率的に無視することができる。ＳＨＡ１の基本的な特性として、動作プログラムを１ビットでも変更すると動作プログラムの特徴量も変更されることと、特徴量の偽造を試みても元の特徴量と同じ特徴量を持つ偽造メッセージを生成できないことの２点が挙げられる。この特性により、動作プログラムと動作プログラムの特徴量が一対一の関係となることが立証される。ＳＨＡ１以外の特徴量の算出方法としては、Massachusetts Institute of TechnologyのRonald Rivest氏が発明したＭＤ５なども挙げられる。なお、動作プログラムファイル２３の特徴量の算出には、ＳＨＡ１、ＭＤ５以外の手法を使用しても良い。また、特徴量算出の実行手段の一例としては、動作プログラムがjava言語で記載されているときには、Sun Microsystems社から提供されているjavaのsecurityパッケージにあるプログラムを使用することによって容易に特徴量を算出できる。

【０１３４】

また、ステップＳ２１で生成した文書情報ファイル２２についても特徴量を算出する（ステップＳ２４：文書情報特徴量算出手段）。文書情報ファイル２２の特徴量算出は、動作プログラムファイル２３の特徴量算出方法と同様な方法で算出すれば良い。

【０１３５】

次いで、秘密鍵・公開鍵を生成し（ステップＳ２５）、生成した秘密鍵で動作プログラムファイル２３の特徴量及び文書情報ファイル２２の特徴量を暗号化する（ステップＳ２６）。秘密鍵を利用した暗号化には、ＲＳＡやＤＳＡ（Digital Signature Algorithm）などを利用する。ＲＳＡの暗号アルゴリズムは大きな数値の素因数分解を実行することが困難であるという事実に依存したものであり、2000ビット以上の係数を持つ鍵であれば安全であると一般的に知られている。ＲＳＡ、ＤＳＡなどは、様々な企業から提供されているため、簡単に使用することが可能である。なお、暗号化に使用する秘密鍵・公開鍵を生成する代わりに、作成者のコンピュータ内に予め保持された秘密鍵・公開鍵を使用するようにしても良い。すなわち、本実施の形態においては、公開鍵暗号方式により動作プログラムファイル２３の特徴量及び文書情報ファイル２２の特徴量を暗号化するものである。

【０１３６】

そして、このように秘密鍵で暗号化された動作プログラムファイル２３の特徴量及び文書情報ファイル２２の特徴量を特徴量保持ファイル２４に保存した後（ステップＳ２７：特徴量保持ファイル生成手段）、文書情報ファイル２２と動作プログラムファイル２３と特徴量保持ファイル２４とを単一の文書としてカプセル化手段を用いてカプセル化したカプセル化文書ファイル２１を作成する（ステップＳ２８）。なお、暗号化された動作プログラムファイル２３の特徴量及び文書情報ファイル２２の特徴量を特徴量保持ファイル２４に保存する際には、動作プログラムファイル２３と暗号化された動作プログラムファイルの特徴量との対応、文書情報ファイル２２と文書情報ファイル２２の特徴量との対応が付くようにしておく。

【０１３７】

以上のようにして作成されたカプセル化文書ファイル２１は、動作プログラムファイル２３の特徴量及び文書情報ファイル２２の特徴量の暗号化に使用された秘密鍵と対になる公開鍵とともに、ネットワーク７を介して所定のコンピュータ１に対して送信されて配布されることになる。

【０１３８】

［２－２．改ざん検証処理］

コンピュータ１は、内蔵するＣＰＵ２がＯＳ内にあるShellプログラムが関連付けされている起動プログラムに従うことにより、動作プログラムファイル２３の改ざん検証処理を実行する改ざん検証装置として機能することになる。ここでは、図１０に示すようなカプセル化文書ファイル２１が公開鍵とともに別のコンピュータ１（カプセル化文書作成装置）から配布されたものとして説明する。

【０１３９】

閲覧者がキーボード１０やマウス１１等の入力装置を介してカプセル化文書ファイル２１を選択した際に、ＯＳ内にあるShellプログラムが拡張子等でカプセル化文書ファイル２１と判断した場合には、起動プログラムが起動する。起動プログラムは、選択されたカプセル化文書ファイル２１を読み込み、カプセル化文書ファイル２１内にある動作プログラムファイル２３の改ざん検証をする。

【０１４０】

図１２は、起動プログラムによる改ざん検証処理の流れを示すフローチャートである。図１２に示すように、まず、配布されたカプセル化文書ファイル２１と公開鍵を取得して解凍すると（ステップＳ３１：読込み手段）、取得した公開鍵を使用してカプセル化文書ファイル２１内にある暗号化された動作プログラムファイル２３の特徴量を復号化する（ステップＳ３２：復号化手段）。

【０１４１】

次いで、ステップＳ３１で取得したカプセル化文書ファイル２１内の動作プログラムファイル２３の特徴量を算出する（ステップＳ３３：特徴量算出手段）。動作プログラムファイル２３の特徴量の算出は、カプセル化文書作成装置での処理と同様に、ＳＨＡ１、ＭＤ５の手法を使用しても良いし、javaのsecurityパッケージにあるプログラムを使用しても良いが、原則的には作成者側と閲覧者側と

の特徴量算出アルゴリズムを一致させることが必要である。前述したように、特徴量保持ファイル２４の特徴量算出情報タグ内の属性情報であるアルゴリズムには、作成者が動作プログラムファイル２３の特徴量を算出した際に使用した特徴量算出アルゴリズムが記載されているので（図５参照）、この特徴量算出アルゴリズム情報に基づいて動作プログラムファイル２３の特徴量の算出を行えば良い。なお、作成者側と閲覧者側との特徴量算出アルゴリズムが対応していれば、必ずしも同一の特徴量算出アルゴリズムで動作プログラムファイル２３の特徴量を算出しなくても良い。

【０１４２】

次いで、ステップＳ３４に進み、配布されたカプセル化文書ファイル２１内の暗号化された動作プログラムファイル２３の特徴量を復号化した値と閲覧者側で動作プログラムファイル２３の特徴量を算出した値とを比較し、動作プログラムファイル２３の改ざん検証を実行する。ここに、改ざん検証実行手段の機能が実行される。ここで、同一の特徴量算出アルゴリズムを使用して同一な動作プログラムファイル２３の特徴量を算出することにより、カプセル化文書ファイル２１内の動作プログラムファイル２３に改ざんがなければ、配布されたカプセル化文書ファイル２１内の暗号化された動作プログラムファイル２３の特徴量を復号化した値と閲覧者側で動作プログラムファイル２３の特徴量を算出した値は一致することになる。したがって、２つの特徴量を比較することにより、動作プログラムファイル２３の改ざんを検証することができる。

【０１４３】

つまり、ステップＳ３２～Ｓ３４において、改ざん検証手段の機能が実行される。

【０１４４】

動作プログラムファイル２３の改ざん検証を行った結果、２つの特徴量が一致していれば、すなわち動作プログラムファイル２３が改ざんされていなければ（ステップＳ３５のＮ）、動作プログラムファイル２３に記載された署名情報をディスプレイ９に表示し（ステップＳ３６）、表示された署名者が信用できるかを閲覧者に判断させる。

【０１４５】

信用できる署名者である旨がキーボード１０やマウス１１等の入力装置を介して閲覧者により入力された場合には（ステップＳ３７のＹ）、動作プログラムファイル２３の文書情報ファイル検証プログラムを起動させる（ステップＳ３８）。

【０１４６】

文書情報ファイル検証プログラムは、取得した公開鍵により暗号化された文書情報ファイル２２の特徴量を復号化し（ステップＳ３９：復号化手段）、文書情報ファイル２２の特徴量を復号化した値と閲覧者側で文書情報ファイル２２の特徴量を算出した値とを比較し、文書情報ファイル２２の改ざん検証を実行する（ステップＳ４０）。つまり、ステップＳ３８～Ｓ４０において、改ざん検証手段の機能が実行される。

【０１４７】

文書情報ファイル２２の改ざん検証を行った結果、２つの特徴量が一致していれば、すなわち文書情報ファイル２２が改ざんされていなければ（ステップＳ４１のＮ）、動作プログラムファイル２３の動作プログラム（文書閲覧プログラム）を起動して文書情報ファイル２２をディスプレイ９に表示する（ステップＳ４２）。

【０１４８】

一方、動作プログラムファイル２３が改ざんされている場合（ステップＳ３５のＹ）、信用できる署名者でない旨がキーボード１０やマウス１１等の入力装置を介して閲覧者により入力された場合（ステップＳ３７のＮ）、文書情報ファイル２２が改ざんされている場合（ステップＳ４１のＹ）、不正なプログラムファイルであることを報知する不正報知処理を実行する（ステップＳ４３）。不正報知処理としては、例えば、カプセル化文書ファイル２１内の動作プログラムファイル２３や文書情報ファイル２２が配布途中で改ざんされたことを通知するダイアログボックスをディスプレイ９上に表示することが考えられる。また、改ざんされたことを作成者側にも通知し、新たにカプセル化文書ファイル２１の配布を要求しても良い。

【０１４９】

このように本実施の形態によれば、カプセル化文書作成装置と改ざん検証装置とを備え、動作プログラムファイル２３全体及び文書情報ファイル２２全体を暗号化処理せずとも、動作プログラムファイル２３の特徴量及び文書情報ファイル２２の特徴量という２０バイト程度の小さなデータを暗号化処理するだけで、カプセル化文書ファイル２１の配布途中における動作プログラムファイル２３及び文書情報ファイル２２の改ざん検証ができる。これにより、高速にカプセル化文書ファイル２１内の動作プログラムファイル２３及び文書情報ファイル２２の改ざん検証が実行できる利便性の高いカプセル化文書ファイル２１を提供することができる。すなわち、動作プログラムファイル２３の改ざん検証のみならず、文書情報ファイル２２の改ざん検証が可能になるので、更に安全に文書を閲覧することが可能になる。

【０１５０】

なお、起動プログラムは、ＯＳ内にあるShellプログラムで起動するものに限るものではなく、Shellプログラムがこの様な機能を有しても良い。

【０１５１】

[第三の実施の形態]

本発明の第三の実施の形態を図１３または図１４に基づいて説明する。なお、本発明の第一の実施の形態または第二の実施の形態において説明した部分と同一部分については同一符号を用い、説明も省略する。

【０１５２】

第一の実施の形態または第二の実施の形態によれば、カプセル化文書ファイル２１内の動作プログラムファイル２３の改ざん検証は可能であるが、動作プログラムファイル２３に記載されている署名情報の信頼性については閲覧者が判断することになる。閲覧者が作成者を既知であれば署名情報に記載された作成者の危険性を判断できるため、カプセル化文書ファイル２１のセキュリティ機能は保たれるが、閲覧者が作成者を既知でないときには作成者の危険性を判断できないため、カプセル化文書ファイル２１のセキュリティ機能が保たれない。そこで、本実施の形態においては、閲覧者が作成者を既知でないときにもカプセル化文書フ

ァイル２１のセキュリティ機能を保つため、作成者側と閲覧者側が信頼できる第三者認証局を設けることによって、カプセル化文書ファイル２１のセキュリティ機能を確保するようにしたものである。

【０１５３】

［１．コンピュータ１が備える特長的な機能の説明］

コンピュータ１が備える特長的な機能について説明する。

【０１５４】

［１－１．カプセル化文書作成処理］

コンピュータ１は、内蔵するＣＰＵ２がＯＳ上で動作するアプリケーションプログラムに従うことにより、カプセル化文書ファイル２１を作成するカプセル化文書作成処理を実行するカプセル化文書作成装置として機能することになる。図１３は、ＣＰＵ２がＯＳ上で動作するアプリケーションプログラムに従うことにより実現されるカプセル化文書作成処理の流れを示すフローチャートである。

【０１５５】

図１３に示すように、まず、作成者の秘密鍵・公開鍵を生成した後（ステップＳ５１）、作成者の身元情報を作成者の公開鍵情報に記載し、作成者の公開鍵情報を第三者認証局へ送信する（ステップＳ５２）。

【０１５６】

ここで、第三者認証局は、公開鍵の正当性を確認し、公開鍵証明書を発行する中立的な機関である。第三者認証局は、作成者の公開鍵情報を取得し、作成者の身元情報を保障するため、作成者の公開鍵情報へ署名情報を記載する。公開鍵の署名方法としては、取得した作成者の公開鍵情報から特徴量を算出し、特徴量を第三者認証局の秘密鍵で暗号化する方法が挙げられる。署名方法は、作成者の信頼性が証明できれば、その他の署名方法を使用しても良い。

【０１５７】

また、第三者認証局は、第三者認証局の秘密鍵情報によって署名した作成者の公開鍵情報を作成者に返信し、第三者認証局の公開鍵情報を閲覧者に安全な通信経路で配布する。ここで安全な経路とは、第三者認証局から閲覧者へ公開鍵を配布する途中で改ざんされないことが保障された経路を示す。第三者認証局の公開

鍵情報の配布形態としては、第三者認証局のホームページ上に掲載して自由にダウンロードできても良いし、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭなどの記憶媒体に公開鍵情報を記録して閲覧者へ配布しても良い。また、第三認証局の公開鍵情報は、閲覧者側のコンピュータに予め保持されている場合が多いので、公開鍵情報を配布せずに閲覧者側のコンピュータに保持されている公開鍵情報を使用しても良い。公開鍵情報のフォーマットとしては、規格化されている認証書フォーマット（Ｘ５０９フォーマットなど）を使用しても良い。これにより、第三者認証局が作成者側の公開鍵情報を署名し、カプセル化文書ファイル２１の信頼性を保証する。

【０１５８】

次に、第三者認証局によって署名された作成者の公開鍵情報を取得する（ステップＳ５３）。

【０１５９】

以降のステップＳ５４～Ｓ５９については、第一の実施の形態で説明した図４に示すステップＳ１～Ｓ３、ステップＳ５～Ｓ７と何ら変わるものではないため、その説明は省略する。

【０１６０】

以上のようにして作成されたカプセル化文書ファイル２１は、第三者認証局によって署名された作成者の公開鍵とともに、ネットワーク７を介して所定のコンピュータ１に対して送信されて配布されることになる。

【０１６１】

［１－２．改ざん検証処理］

コンピュータ１は、内蔵するＣＰＵ２がＯＳ内にあるShellプログラムが関連付けされている起動プログラムに従うことにより、動作プログラムファイル２３の改ざん検証処理を実行する改ざん検証装置として機能することになる。ここでは、図３に示すようなカプセル化文書ファイル２１が第三者認証局によって署名された作成者の公開鍵とともに別のコンピュータ１（カプセル化文書作成装置）から配布されたものとして説明する。また、第三者認証局の公開鍵情報が、閲覧者に安全な通信経路で配布されているものとする。

【０１６２】

閲覧者がキーボード１０やマウス１１等の入力装置を介してカプセル化文書ファイル２１を選択した際に、ＯＳ内にあるShellプログラムが拡張子等でカプセル化文書ファイル２１と判断した場合には、起動プログラムが起動する。起動プログラムは、選択されたカプセル化文書ファイル２１を読み込み、カプセル化文書ファイル２１内にある動作プログラムファイル２３の改ざん検証をする。

【０１６３】

図１４は、起動プログラムによる改ざん検証処理の流れを示すフローチャートである。図１４に示すように、まず、配布されたカプセル化文書ファイル２１と第三者認証局によって署名された作成者の公開鍵を取得して解凍すると（ステップＳ６１）、第三者認証局の公開鍵を使用して、暗号化された作成者の公開鍵情報を復号化し（ステップＳ６２）、作成者の公開鍵に記載されている署名情報を検証する（ステップＳ６３）。

【０１６４】

第三者認証局によって保証されている場合、つまり改ざんされていない場合には（ステップＳ６４のＮ）、復号化された作成者の公開鍵を使用してカプセル化文書ファイル２１内にある暗号化された動作プログラムファイル２３の特徴量を復号化し（ステップＳ６５）、動作プログラムファイル２３の特徴量を算出する（ステップＳ６６）。

【０１６５】

次いで、ステップＳ６７に進み、配布されたカプセル化文書ファイル２１内の暗号化された動作プログラムファイル２３の特徴量を復号化した値と閲覧者側で動作プログラムファイル２３の特徴量を算出した値とを比較し、動作プログラムファイル２３の改ざん検証を実行する。

【０１６６】

動作プログラムファイル２３の改ざん検証を行った結果、２つの特徴量が一致していれば、すなわち動作プログラムファイル２３が改ざんされていなければ（ステップＳ６８のＮ）、動作プログラムファイル２３に記載された署名情報をディスプレイ９に表示し（ステップＳ６９）、表示された署名者が信用できるかを

閲覧者に判断させる。

【０１６７】

信用できる署名者である旨がキーボード１０やマウス１１等の入力装置を介して閲覧者により入力された場合には（ステップＳ７０のＹ）、動作プログラムファイル２３の動作プログラムを実行してディスプレイ９上にカプセル化文書ファイル２１内の文書情報ファイル２２を表示する（ステップＳ７１）。

【０１６８】

一方、第三者認証局によって保証されていない場合（ステップＳ６４のＹ）、動作プログラムファイル２３が改ざんされている場合（ステップＳ６８のＹ）、信用できる署名者でない旨がキーボード１０やマウス１１等の入力装置を介して閲覧者により入力された場合には（ステップＳ７０のＮ）、動作プログラムファイル２３の動作プログラムを実行せずに、不正なプログラムファイルであることを報知する不正報知処理を実行する（ステップＳ７２）。不正報知処理としては、例えば、公開鍵が第三者認証局によって保証されていない旨やカプセル化文書ファイル２１内の動作プログラムファイル２３が配布途中で改ざんされたことを通知するダイアログボックスをディスプレイ９上に表示することが考えられる。

【０１６９】

このように本実施の形態によれば、カプセル化文書作成装置と改ざん検証装置とを備え、動作プログラムファイル２３全体を暗号化処理せずとも、動作プログラムファイル２３の特徴量という２０バイト程度の小さなデータを暗号化処理するだけで、カプセル化文書ファイル２１の配布途中における動作プログラムファイル２３の改ざん検証ができる。これにより、高速にカプセル化文書ファイル２１内の動作プログラムファイル２３の改ざん検証が実行できる利便性の高いカプセル化文書ファイル２１を提供することができる。また、第三者認証局が作成者側の公開鍵情報を署名し、カプセル化文書ファイル２１の信頼性を保証することにより、閲覧者が作成者を既知でなくとも作成者の危険性を判定してカプセル化文書ファイル２１のセキュリティ機能を保つことができる。

【０１７０】

なお、起動プログラムは、ＯＳ内にあるShellプログラムで起動するものに限

るものではなく、Shellプログラムがこの様な機能を有しても良い。

【０１７１】

なお、本実施の形態においては、作成者の公開鍵情報の特徴量を暗号化することによって、カプセル化文書ファイル２１の安全性を保証したが、作成者の公開鍵情報を暗号化することによって、カプセル化文書ファイル２１の安全性を保証するようにしても良い。

【０１７２】

一例として、オペレーティングシステム（ＯＳ）提供者が、作成者の公開鍵情報を暗号化する例を以下に示す。

【０１７３】

まず、ＯＳ提供者が、ＯＳ提供者の秘密鍵・公開鍵情報を作成し、作成者の公開鍵情報をＯＳ提供者の秘密鍵で暗号化して、暗号化した作成者の公開鍵を作成者へ返信する。なお、ＯＳ提供者の公開鍵情報は、ＯＳに予め保存されている。

【０１７４】

作成者は、作成したカプセル化文書ファイル２１と暗号化された公開鍵情報を閲覧者へ送信する。

【０１７５】

閲覧者は、ＯＳに予め保存されているＯＳ提供者の公開鍵情報を使用して、暗号化された公開鍵情報を復号化し、復号化された公開鍵情報を使用して、カプセル化文書ファイル２１の動作プログラムファイル２３を第一の実施の形態と同様に検証することによって、安全にカプセル化文書ファイル２１を使用することができる。

【０１７６】

作成者の公開鍵情報を暗号化する方法では、公開鍵情報が第三者の秘密鍵によって暗号化されているので、閲覧者は第三者の公開鍵情報を取得しないと、作成者の公開鍵情報を使用できないため、カプセル化文書を利用することができない。このため、作成者の公開鍵情報を暗号化する方法では、作成者は第三者を通して、閲覧者に対して課金処理などを行うことも可能となる。

【０１７７】

一方、作成者の公開鍵情報の特徴量を暗号化する方法では、公開鍵情報は第三者の秘密鍵によって暗号化されていないので、作成者の公開鍵情報の署名情報が第三者によって証明されなくとも、閲覧者は作成者の公開鍵情報を使用するか否かの選択をして、カプセル化文書ファイル２１を使用することが可能となる。

【０１７８】

［第四の実施の形態］

本発明の第四の実施の形態を図１５または図１６に基づいて説明する。なお、本発明の第一の実施の形態ないし第三の実施の形態において説明した部分と同一部分については同一符号を用い、説明も省略する。

【０１７９】

第一の実施の形態ないし第三の実施の形態によれば、各動作プログラムファイル２３の特徴量が暗号化されて保存されている特徴量保持ファイル２４をカプセル化文書ファイル２１に保持するようにしたが、本実施の形態においては、特徴量保持ファイル２４をカプセル化文書ファイル２１に保持せずに、ＯＳ内にあるShellプログラムが関連付けされている起動プログラムに保持するようにしたものである。

【０１８０】

［１．カプセル化文書の説明］

本発明の特長の１つである文書のデータ構造（カプセル化文書構造）の概要について図１５を参照して説明する。このカプセル化文書ファイル２１は、コンピュータ１のＨＤＤ５に保持されている。本実施の形態のカプセル化文書ファイル２１は、文書上での表現実体となる各種のコンテンツや文書構造をファイル化した文書情報ファイル２２と、文書情報ファイル２２を表現実体化させる動作プログラムの動作プログラムファイル２３とを、単一の文書としてカプセル化手段を用いてカプセル化したものである。これらの情報は、各々一般的なコンピュータ１のＯＳが管理できる個別のファイル単位の構造となっている。

【０１８１】

より詳細には、文書情報ファイル２２のコンテンツ情報は、静止画像、動画像、音声、テキストファイル等であってコンピュータ１で使用、動作出来るファイ

ルフォーマットに準じてファイル化されている。また、カプセル化手段には、ＺＩＰ、ＬＨＡ等の周知のマルチファイル圧縮方式を使用し、各文書情報ファイル２２を閲覧等で表示する場合はこれらのマルチファイル圧縮フォーマットで符号化されているファイルを動的に復号化することで使用する。

【０１８２】

動作プログラムファイル２３の動作プログラムは、中間言語コードで記述されている事が望ましい。動作プログラムが中間言語で記述されていれば、この中間言語を解釈実行できるコンパイラまたはインタプリタプログラムがコンピュータにインストールされている状況においてコンピュータの機種依存性が無くなる。このような中間言語としては、java（Sun Microsystemsの登録商標）言語がある。このような動作プログラムファイル２３の特徴量は、起動プログラムに保持されている。

【０１８３】

すなわち、第一の実施の形態ないし第三の実施の形態のカプセル化文書ファイル２１と異なる点は、特徴量保持ファイル２４をカプセル化文書ファイル２１に保持していない点である。

【０１８４】

したがって、文書情報ファイル２２を表現実体化させる動作プログラムファイル２３が当該文書情報ファイル２２と一体にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、配布された動作プログラムファイル２３の特徴量を算出し、外部に保持されている動作プログラムファイル２３の特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイル２１の配布途中における動作プログラムファイル２３の改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【０１８５】

［２．コンピュータ１が備える特長的な機能の説明］

次に、コンピュータ１が備える特長的な機能について説明する。

【０１８６】

［２－１．改ざん検証処理］

コンピュータ１は、内蔵するＣＰＵ２がＯＳ内にあるShellプログラムが関連付けされている起動プログラムに従うことにより、動作プログラムファイル２３の改ざん検証処理を実行する改ざん検証装置として機能することになる。ここでは、図１５に示すようなカプセル化文書ファイル２１が公開鍵とともに別のコンピュータ１（カプセル化文書作成装置）から配布されたものとして説明する。

【０１８７】

閲覧者がキーボード１０やマウス１１等の入力装置を介してカプセル化文書ファイル２１を選択した際に、ＯＳ内にあるShellプログラムが拡張子等でカプセル化文書ファイル２１と判断した場合には、起動プログラムが起動する。起動プログラムは、選択されたカプセル化文書ファイル２１を読み込み、カプセル化文書ファイル２１内にある動作プログラムファイル２３の改ざん検証をする。

【０１８８】

図１６は、起動プログラムによる改ざん検証処理の流れを示すフローチャートである。図１６に示すように、まず、起動プログラム内の動作プログラムファイル２３の特徴量を読み込む（ステップＳ８１）。

【０１８９】

次に、閲覧者がキーボード１０やマウス１１等の入力装置を介して選択したカプセル化文書ファイル２１内にある動作プログラムファイル２３を読み込み（ステップＳ８２）、動作プログラムファイル２３の特徴量を算出する（ステップＳ８３）。

【０１９０】

次いで、ステップＳ８４に進み、起動プログラム内の動作プログラムファイル２３の特徴量と閲覧者側で算出した動作プログラムファイル２３の特徴量とを比較し、動作プログラムファイル２３の改ざん検証を実行する。

【０１９１】

動作プログラムファイル２３の改ざん検証を行った結果、２つの特徴量が一致している場合、すなわち動作プログラムファイル２３が改ざんされていない場合には（ステップＳ８５のＮ）、動作プログラムファイル２３の動作プログラム（

文書閲覧プログラム）を起動して文書情報ファイル２２をディスプレイ９に表示する（ステップＳ８６）。

【０１９２】

一方、特徴量検証プログラムファイルの改ざん検証を行った結果、２つの特徴量が一致していない場合、すなわち特徴量検証プログラムファイルが改ざんされている場合には（ステップＳ８５のＹ）、特徴量検証プログラムファイルが改ざんされたことを報知する不正報知処理を実行する（ステップＳ８７）。不正報知処理としては、例えば、特徴量検証プログラムファイルが改ざんされたことを通知するダイアログボックスをディスプレイ９上に表示することが考えられる。

【０１９３】

このように本実施の形態によれば、カプセル化文書作成装置と改ざん検証装置とを備え、動作プログラムファイル２３全体を暗号化処理せずとも、カプセル化文書ファイル２１の配布途中における動作プログラムファイル２３の改ざん検証ができる。これにより、高速にカプセル化文書ファイル２１内の動作プログラムファイル２３の改ざん検証が実行できる利便性の高いカプセル化文書ファイル２１を提供することができる。

【０１９４】

なお、起動プログラムは、ＯＳ内にあるShellプログラムで起動するものに限るものではなく、Shellプログラムがこの様な機能を有しても良い。

【０１９５】

また、起動プログラムがＯＳのＳｈｅｌｌプログラムの機能としてない場合は、閲覧者がカプセル化文書ファイル２１を起動するために起動プログラムを取得することが必須となる。起動プログラムの取得方法としては、起動プログラムをインターネットからダウンロードするようにすることが考えられる。しかしながら、インターネットから起動プログラムをダウンロードする場合は、起動プログラムをダウンロードするサイトのＵＲＬを使用者が知らなければならない。そこで、このファイルのプロパティ情報としてＵＲＬを記述しておいても良いし、ファイルの先頭にＵＲＬを記述することによって、汎用のテキストエディタでも容易に起動プログラムのダウンロードサイトのＵＲＬを認識できるようにしても良

い。

【０１９６】

［第五の実施の形態］

本発明の第五の実施の形態を図１７ないし図１９に基づいて説明する。なお、本発明の第一の実施の形態ないし第三の実施の形態において説明した部分と同一部分については同一符号を用い、説明も省略する。

【０１９７】

［１．カプセル化文書の説明］

本発明の特長の１つである文書のデータ構造（カプセル化文書構造）の概要について図１７を参照して説明する。このカプセル化文書ファイル２１は、コンピュータ１のＨＤＤ５に保持されている。本実施の形態のカプセル化文書ファイル２１は、文書上での表現実体となる各種のコンテンツや文書構造をファイル化した文書情報ファイル２２と、文書情報ファイル２２を表現実体化させる動作プログラムの動作プログラムファイル２３と、特徴量検証プログラムファイル２５とを、単一の文書としてカプセル化手段を用いてカプセル化したものである。これらの情報は、各々一般的なコンピュータ１のＯＳが管理できる個別のファイル単位の構造となっている。

【０１９８】

より詳細には、文書情報ファイル２２のコンテンツ情報は、静止画像、動画像、音声、テキストファイル等であってコンピュータ１で使用、動作出来るファイルフォーマットに準じてファイル化されている。また、カプセル化手段には、ＺＩＰ、ＬＨＡ等の周知のマルチファイル圧縮方式を使用し、各文書情報ファイル２２を閲覧等で表示する場合はこれらのマルチファイル圧縮フォーマットで符号化されているファイルを動的に復号化することで使用する。

【０１９９】

動作プログラムファイル２３の動作プログラムは、中間言語コードで記述されている事が望ましい。動作プログラムが中間言語で記述されていれば、この中間言語を解釈実行できるコンパイラまたはインタプリタプログラムがコンピュータにインストールされている状況においてコンピュータの機種依存性が無くなる。

このような中間言語としては、java（Sun Microsystemsの登録商標）言語がある。

【０２００】

特徴量検証プログラムファイル２５は、動作プログラムファイル２３の改ざん検証を実行するものである。このような特徴量検証プログラムファイルの特徴量は、起動プログラムに保持されている。

【０２０１】

すなわち、第一の実施の形態ないし第三の実施の形態のカプセル化文書ファイル２１と異なる点は、特徴量検証プログラムファイル２５をカプセル化文書ファイル２１に保持している点である。

【０２０２】

［２．コンピュータ１が備える特長的な機能の説明］

次に、コンピュータ１が備える特長的な機能について説明する。本実施の形態の特長的な処理は、カプセル化文書ファイル２１に保持されている特徴量検証プログラムファイル２５を外部の起動プログラムから起動して動作させることにより、動作プログラムファイル２３の改ざん検証処理を実行するものである。

【０２０３】

［２－１．改ざん検証処理］

コンピュータ１は、内蔵するＣＰＵ２がＯＳ内にあるShellプログラムが関連付けされている起動プログラムに従うことにより、動作プログラムファイル２３の改ざん検証処理を実行する改ざん検証装置として機能することになる。ここでは、図１７に示すようなカプセル化文書ファイル２１が公開鍵とともに別のコンピュータ１（カプセル化文書作成装置）から配布されたものとして説明する。

【０２０４】

閲覧者がキーボード１０やマウス１１等の入力装置を介してカプセル化文書ファイル２１を選択した際に、ＯＳ内にあるShellプログラムが拡張子等でカプセル化文書ファイル２１と判断した場合には、起動プログラムが起動する。起動プログラムは、選択されたカプセル化文書ファイル２１を読み込み、カプセル化文書ファイル２１内にある動作プログラムファイル２３の改ざん検証をする。

【０２０５】

図１８は、起動プログラムによる改ざん検証処理の流れを示すフローチャートである。図１８に示すように、まず、起動プログラム内の特徴量検証プログラムファイル２５の特徴量を読み込む（ステップＳ９１）。

【０２０６】

次に、閲覧者がキーボード１０やマウス１１等の入力装置を介して選択したカプセル化文書ファイル２１内にある特徴量検証プログラムファイル２５を読み込み（ステップＳ９２）、特徴量検証プログラムファイル２５の特徴量を算出する（ステップＳ９３：特徴量算出手段）。

【０２０７】

次いで、ステップＳ９４に進み、起動プログラム内の特徴量検証プログラムファイル２５の特徴量と閲覧者側で算出した特徴量検証プログラムファイル２５の特徴量とを比較し、特徴量検証プログラムファイル２５の改ざん検証を実行する。

【０２０８】

特徴量検証プログラムファイル２５の改ざん検証を行った結果、２つの特徴量が一致している場合、すなわち特徴量検証プログラムファイル２５が改ざんされていない場合には（ステップＳ９５のＮ：判定手段）、特徴量検証プログラムを実行する（ステップＳ９６：改ざん検証実行手段）。

【０２０９】

一方、特徴量検証プログラムファイル２５の改ざん検証を行った結果、２つの特徴量が一致していない場合、すなわち特徴量検証プログラムファイル２５が改ざんされている場合には（ステップＳ９５のＹ：判定手段）、特徴量検証プログラムファイル２５が改ざんされたことを報知する不正報知処理を実行する（ステップＳ９７）。不正報知処理としては、例えば、特徴量検証プログラムファイル２５が改ざんされたことを通知するダイアログボックスをディスプレイ９上に表示することが考えられる。

【０２１０】

ここで、ステップＳ９６での特徴量検証プログラムを実行することにより実現

される特徴量検証処理について説明する。図１９は、特徴量検証処理の流れを示すフローチャートである。図１９に示すように、まず、同じカプセル化文書ファイル２１内の動作プログラムファイル２３及び特徴量保持ファイル２４をすべて読み込み（ステップＳ１０１）、取得した公開鍵を使用して暗号化された特徴量を復号化するとともに（ステップＳ１０２）、動作プログラムファイル２３の特徴量を算出する（ステップＳ１０３）。

【０２１１】

次いで、ステップＳ１０４に進み、復号化した動作プログラムファイル２３の特徴量と閲覧者側で算出した動作プログラムファイル２３の特徴量とを比較し、動作プログラムファイル２３の改ざん検証を実行する。

【０２１２】

動作プログラムファイル２３の改ざん検証を行った結果、２つの特徴量が一致している場合、すなわち動作プログラムファイル２３が改ざんされていない場合には（ステップＳ１０５のＮ）、動作プログラムファイル２３の動作プログラム（文書閲覧プログラム）を起動して文書情報ファイル２２をディスプレイ９に表示する（ステップＳ１０６）。

【０２１３】

一方、動作プログラムファイル２３の改ざん検証を行った結果、２つの特徴量が一致していない場合、すなわち動作プログラムファイル２３が改ざんされている場合には（ステップＳ１０５のＹ）、動作プログラムファイル２３が改ざんされたことを報知する不正報知処理を実行する（ステップＳ１０７）。不正報知処理としては、例えば、動作プログラムファイル２３が改ざんされたことを通知するダイアログボックスをディスプレイ９上に表示することが考えられる。

【０２１４】

このように本実施の形態によれば、カプセル化文書ファイル２１内に特徴量検証プログラムファイル２５を挿入し、起動プログラムが特徴量検証プログラムファイル２５の改ざん検証と特徴量検証プログラム２５の起動とを実行することにより、カプセル化文書ファイル２１内にある複数の動作プログラムファイル２３の全てに対して改ざん検証を行うことが可能となる。

【０２１５】

なお、起動プログラムは、ＯＳ内にあるＳｈｅｌｌプログラムで起動するものに限るものではなく、Ｓｈｅｌｌプログラムがこの様な機能を有しても良い。

【０２１６】

また、起動プログラムがＯＳのＳｈｅｌｌプログラムの機能としてない場合は、閲覧者がカプセル化文書ファイル２１を起動するために起動プログラムを取得することが必須となる。起動プログラムの取得方法としては、起動プログラムをインターネットからダウンロードするようにすることが考えられる。しかしながら、インターネットから起動プログラムをダウンロードする場合は、起動プログラムをダウンロードするサイトのＵＲＬを使用者が知らなければならない。そこで、このファイルのプロパティ情報としてＵＲＬを記述しておいても良いし、ファイルの先頭にＵＲＬを記述することによって、汎用のテキストエディタでも容易に起動プログラムのダウンロードサイトのＵＲＬを認識できるようにしても良い。

【０２１７】

なお、各実施の形態においては、暗号化と復号化の鍵情報が異なる公開鍵暗号方式により動作プログラムファイル２３の特徴量等を暗号化するようにしたが、これに限るものではなく、暗号化と復号化の鍵情報が同一である秘密鍵暗号方式により動作プログラムファイル２３の特徴量等を暗号化するようにしても良い。すなわち、カプセル化文書ファイル２１を閲覧する閲覧者のコンピュータ１には、動作プログラムファイル２３の特徴量等を暗号化した鍵情報が保持されることになる。したがって、各閲覧者のコンピュータ１には、異なる鍵情報が必要となる。なお、この鍵情報は秘密にすることが前提なので、カプセル化文書ファイル２１内に鍵情報を添付して配布することはできない。これにより、暗号化鍵と復号化鍵とが同一の鍵であることにより、暗号化や復号化を高速に実行することが可能になる。

【０２１８】

【発明の効果】

請求項１記載の発明のプログラム改ざん検証方法によれば、動作プログラムファイル全体を暗号化処理せずとも、動作プログラムファイルの特徴量という小さ

なデータ（２０バイト程度）を暗号化処理するだけで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が行えるので、動作プログラムファイルの改ざん検証を高速に行うことができる。

【０２１９】

請求項２記載の発明のプログラム改ざん検証方法によれば、動作プログラムファイル全体を暗号化処理せずとも、動作プログラムファイルの特徴量という小さなデータ（２０バイト程度）を暗号化処理するだけで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が行えるので、動作プログラムファイルの改ざん検証を高速に行うことができる。

【０２２０】

請求項３記載の発明のカプセル化文書構造によれば、各種ファイルで構成されるファイル群とファイル群を構成する所定のファイルに関する暗号化された特徴量を保持する特徴量保持ファイルとが一元的に管理されていることにより、カプセル化文書ファイルを配布する際に、所定のファイルの暗号化特徴量を復号化するとともに配布された所定のファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中におけるファイルの改ざん検証を行うことができる。

【０２２１】

請求項４記載の発明のカプセル化文書構造によれば、文書情報ファイルを表現実体化させる動作プログラムファイルが当該文書情報ファイルと一体にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することができ、この際、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証ができるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【０２２２】

請求項５記載の発明のカプセル化文書構造によれば、文書情報ファイルを表現

実体化させる動作プログラムファイルの保存位置を示す位置情報が当該文書情報ファイルと一体にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することができ、この際、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに所定位置に保存されている動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【０２２３】

請求項６記載の発明のカプセル化文書構造によれば、文書情報ファイルを表現実体化させる動作プログラムファイルが当該文書情報ファイルと一体にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することができ、この際、配布された動作プログラムファイルの特徴量を算出し、外部に保持されている動作プログラムファイルの特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【０２２４】

請求項７記載の発明のカプセル化文書構造によれば、文書情報ファイルを表現実体化させる動作プログラムファイルの保存位置を示す位置情報が当該文書情報のファイルと一体にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することができ、この際、所定位置に保存されている動作プログラムファイルの特徴量を算出し、外部に保持されている動作プログラムファイルの特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証ができるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【０２２５】

請求項８記載の発明によれば、請求項３ないし５の何れか一記載のカプセル化

文書構造において、前記特徴量保持ファイルには、前記文書情報ファイルに関する暗号化された特徴量も保持されていることにより、動作プログラムファイルの改ざん検証のみならず、文書情報ファイルの改ざん検証が可能になるので、更に安全に文書を閲覧することができる。

【０２２６】

請求項９記載の発明によれば、請求項３ないし５の何れか一記載のカプセル化文書構造において、前記特徴量保持ファイルには、前記動作プログラムファイルに関する暗号化された特徴量に対応付けられて前記暗号化された特徴量を復号化する復号化鍵情報が保持されていることにより、閲覧者はカプセル化文書ファイルを取得するだけで動作プログラムファイル等の改ざん検証を行うことができる。

【０２２７】

請求項１０記載の発明によれば、請求項３ないし５の何れか一記載のカプセル化文書構造において、前記特徴量保持ファイルには、前記動作プログラムファイルに関する暗号化された特徴量に対応付けられて前記暗号化された特徴量を復号化する復号化鍵情報の保存位置を示す位置情報が保持されていることにより、閲覧者はカプセル化文書ファイルを取得するだけで動作プログラムファイル等の改ざん検証を行うことができる。

【０２２８】

請求項１１記載の発明によれば、請求項９または１０記載のカプセル化文書構造において、各動作プログラムファイル毎に異なる前記復号化鍵情報が対応付けられていることにより、例えば１つのベンダーだけでなく複数のベンダーによって複数の動作プログラムファイルが作成されるような場合、閲覧者は、各ベンダーの復号化鍵情報を使用することによって動作プログラムファイルの改ざん検証を行うことができるので、ベンダーごとに作成した動作プログラムファイルに対して、責任を持たせることが可能なカプセル化文書ファイルを提供することができる。

【０２２９】

請求項１２記載の発明によれば、請求項３ないし１１の何れか一記載のカプセ

ル化文書構造において、前記動作プログラムファイルに関する特徴量は、公開鍵暗号方式により暗号化されていることにより、カプセル化文書ファイルの生成者が所有して公開しない秘密鍵を暗号化鍵とし、秘密鍵とは異なる公開鍵を復号化鍵として閲覧者に公開することで、公開鍵を有する者だけが動作プログラムファイルに関する特徴量を復号化することができる。

【０２３０】

請求項１３記載の発明によれば、請求項１２記載のカプセル化文書構造において、前記復号化鍵情報は、第三者認証局により署名暗号化されていることにより、第三者認証局が作成者側の復号化鍵情報（公開鍵情報）を署名し、カプセル化文書ファイルの信頼性を保証することで、閲覧者が作成者を既知でなくとも作成者の危険性を判定してカプセル化文書ファイルのセキュリティ機能を保つことができる。

【０２３１】

請求項１４記載の発明によれば、請求項３ないし１１の何れか一記載のカプセル化文書構造において、前記動作プログラムファイルに関する特徴量は、秘密鍵暗号方式により暗号化されていることにより、暗号化鍵と復号化鍵とが同一の鍵であるので、暗号化や復号化を高速に実行することができる。

【０２３２】

請求項１５記載の発明によれば、請求項３ないし１４の何れか一記載のカプセル化文書構造において、カプセル化文書ファイル内に特徴量検証プログラムファイルを挿入し、起動プログラムが特徴量検証プログラムファイルの改ざん検証と特徴量検証プログラムの起動とを実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことができる。

【０２３３】

請求項１６記載の発明の記憶媒体によれば、請求項３ないし１５の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを格納したことにより、請求項３ないし１５の何れか一記載の発明と同様の作用効果を奏する。

【０２３４】

請求項１７記載の発明のカプセル化文書作成装置によれば、セキュリティ性の高い請求項４記載のファイル構造のカプセル化文書ファイルを簡単に作成することができる。

【０２３５】

請求項１８記載の発明によれば、請求項１７記載のカプセル化文書作成装置において、セキュリティ性の高い請求項８記載のファイル構造のカプセル化文書ファイルを簡単に作成することができる。

【０２３６】

請求項１９記載の発明の改ざん検証装置によれば、請求項３ないし１５の何れか一記載のカプセル化文書構造のカプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、動作プログラムファイルの改ざん検証を実行することにより、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証ができるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【０２３７】

請求項２０記載の発明によれば、請求項１９記載の改ざん検証装置において、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【０２３８】

請求項２１記載の発明によれば、請求項１９記載の改ざん検証装置において、配布された動作プログラムファイルの特徴量を算出し、起動プログラム内の特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【０２３９】

請求項２２記載の発明によれば、請求項１９記載の改ざん検証装置において、配布された動作プログラムファイルの特徴量を算出するとともに算出された動作

プログラムファイルの特徴量を暗号化し、この暗号化した特徴量と特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【０２４０】

請求項２３記載の発明によれば、請求項１９記載の改ざん検証装置において、配布されたカプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出し、起動プログラム内の特徴量検証プログラムファイル特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における特徴量検証プログラムファイルの改ざん検証が可能になり、改ざんがなされていない場合に特徴量検証プログラムの起動を実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことができる。

【０２４１】

請求項２４記載の発明のカプセル化文書作成処理プログラムによれば、セキュリティ性の高い請求項４記載のファイル構造のカプセル化文書ファイルを簡単に作成することができる。

【０２４２】

請求項２５記載の発明によれば、請求項２４記載のカプセル化文書作成処理プログラムにおいて、セキュリティ性の高い請求項８記載のファイル構造のカプセル化文書ファイルを簡単に作成することができる。

【０２４３】

請求項２６記載の発明の記憶媒体によれば、請求項２４または２５記載のカプセル化文書作成処理プログラムを記憶することにより、この記憶媒体に記憶されたカプセル化文書作成処理プログラムをコンピュータに読み取らせることで、セキュリティ性の高い請求項４または８記載のファイル構造のカプセル化文書ファイルを簡単に作成することができる。

【０２４４】

請求項２７記載の発明の起動プログラムによれば、請求項３ないし１５の何れ

か一記載のカプセル化文書構造のカプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、動作プログラムファイルの改ざん検証を実行することにより、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証ができるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【０２４５】

請求項２８記載の発明によれば、請求項２７記載の起動プログラムにおいて、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【０２４６】

請求項２９記載の発明によれば、請求項２７記載の起動プログラムにおいて、配布された動作プログラムファイルの特徴量を算出し、起動プログラム内の特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【０２４７】

請求項３０記載の発明によれば、請求項２７記載の起動プログラムにおいて、配布された動作プログラムファイルの特徴量を算出するとともに算出された動作プログラムファイルの特徴量を暗号化し、この暗号化した特徴量と特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【０２４８】

請求項３１記載の発明によれば、請求項２７記載の起動プログラムにおいて、配布されたカプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出し、起動プログラム内の特徴量検証プログラムファイル特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配

布途中における特徴量検証プログラムファイルの改ざん検証を行うことができ、改ざんがなされていない場合に特徴量検証プログラムの起動を実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことができる。

【０２４９】

請求項３２記載の発明の記憶媒体によれば、請求項２７ないし３１のいずれか一記載の起動プログラムを記憶することにより、この記憶媒体に記憶されたカプセル化文書作成処理プログラムをコンピュータに読み取らせることで、請求項２７ないし３１のいずれか一記載の発明と同様の作用効果を奏する。

【図面の簡単な説明】

【図１】

本発明の第一の実施の形態も適用される一般的又は標準的なパーソナルコンピュータを示すハードウェア構成図である。

【図２】

ＯＳの役割の概要を示す模式図である。

【図３】

カプセル化文書ファイルのデータ構造を示す模式図である。

【図４】

カプセル化文書作成処理の流れを示すフローチャートである。

【図５】

特徴量保持ファイルの例を示す説明図である。

【図６】

改ざん検証処理の流れを示すフローチャートである。

【図７】

動作権限の種類と動作権限モードとの対応関係を示す説明図である。

【図８】

特徴量保持ファイルの例を示す説明図である。

【図９】

特徴量保持ファイルの例を示す説明図である。

【図１０】

本発明の第二の実施の形態のカプセル化文書ファイルのデータ構造を示す模式図である。

【図１１】

カプセル化文書作成処理の流れを示すフローチャートである。

【図１２】

改ざん検証処理の流れを示すフローチャートである。

【図１３】

本発明の第三の実施の形態のカプセル化文書作成処理の流れを示すフローチャートである。

【図１４】

改ざん検証処理の流れを示すフローチャートである。

【図１５】

本発明の第四の実施の形態のカプセル化文書ファイルのデータ構造を示す模式図である。

【図１６】

改ざん検証処理の流れを示すフローチャートである。

【図１７】

本発明の第五の実施の形態のカプセル化文書ファイルのデータ構造を示す模式図である。

【図１８】

改ざん検証処理の流れを示すフローチャートである。

【図１９】

特徴量検証処理の流れを示すフローチャートである。

【符号の説明】

１	カプセル化文書作成装置、改ざん検証装置
２	情報処理部
６	記憶媒体
２１	カプセル化文書ファイル

２２　　文書情報ファイル

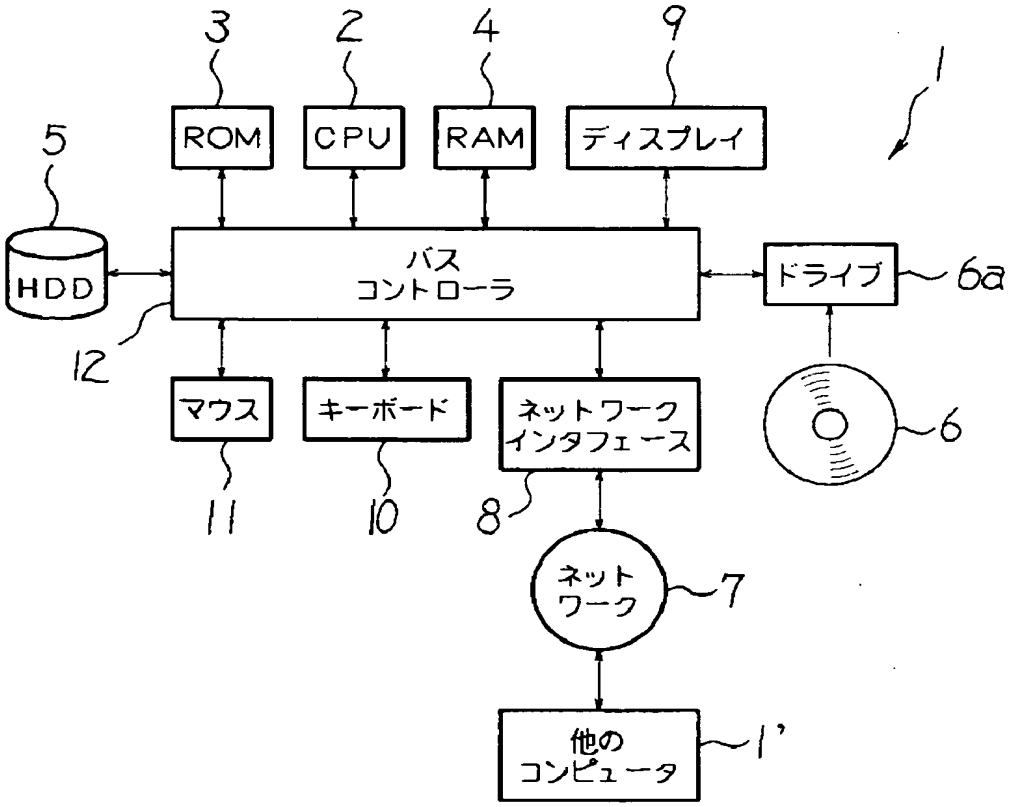
２３　　動作プログラムファイル

２４　　特徴量保持ファイル

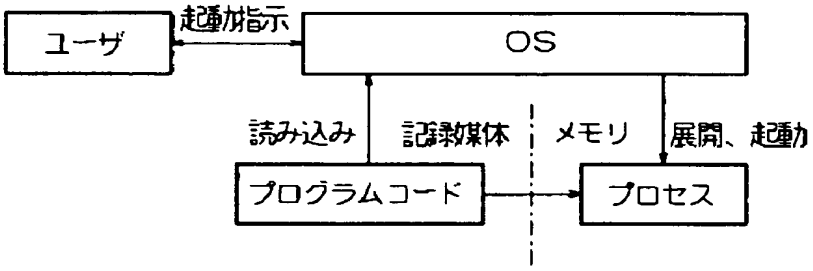
２５　　特徴量検証プログラムファイル

【書類名】　図面

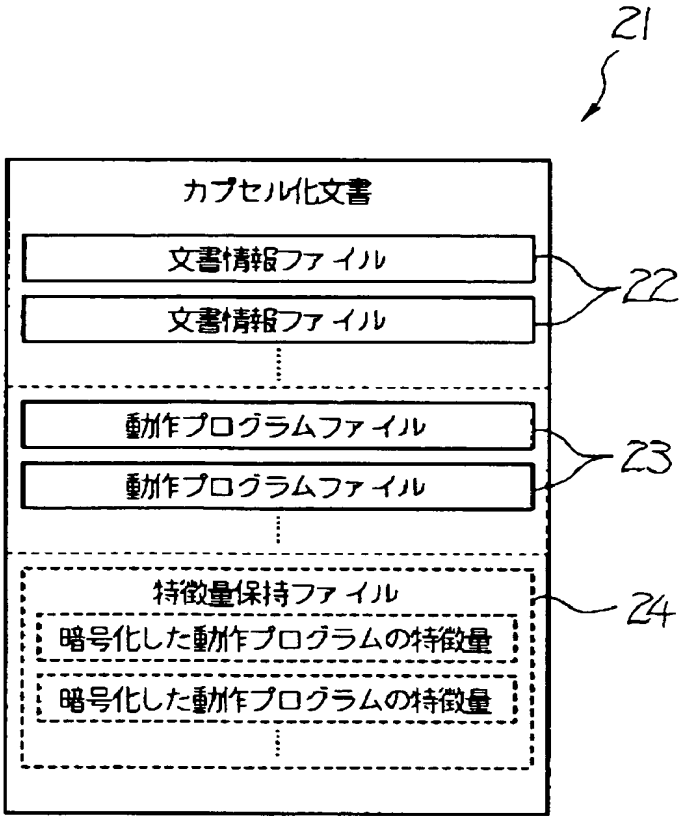
【図１】


3
2
4
9
1
5
ROM
CPU
RAM
ディスプレイ
HDD
バス
コントローラ
ドライブ
6a
12
マウス
キーボード
ネットワーク
インタフェース
6
11
10
8
ネット
ワーク
7
他の
コンピュータ
1'

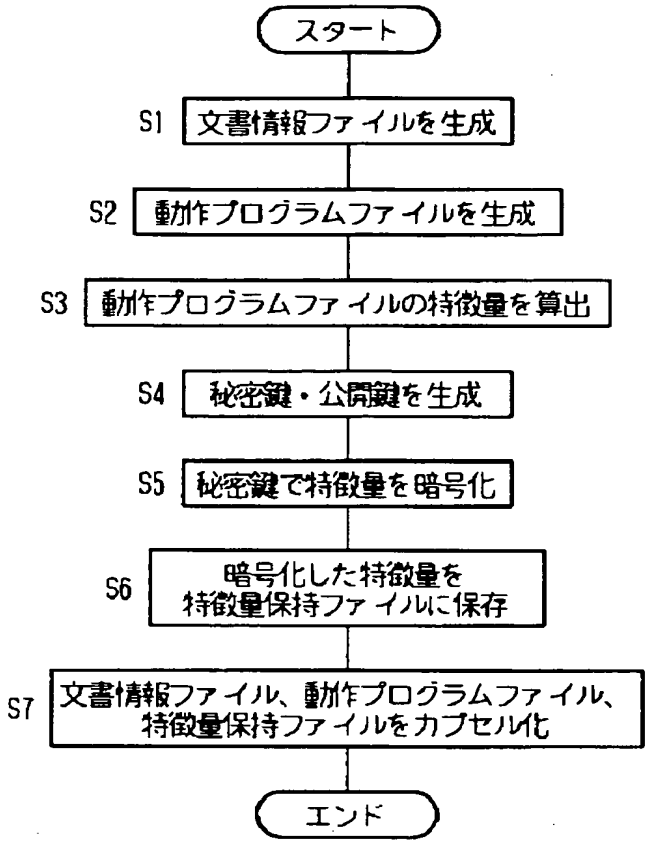
【図２】


ユーザ
起動指示
OS
読み込み
記録媒体
メモリ
展開、起動
プログラムコード
プロセス

【図３】


21
カプセル化文書
文書情報ファイル
文書情報ファイル
22
動作プログラムファイル
動作プログラムファイル
23
特徴量保持ファイル
暗号化した動作プログラムの特徴量
暗号化した動作プログラムの特徴量
24

【図４】


スタート
S1
文書情報ファイルを生成
S2
動作プログラムファイルを生成
S3
動作プログラムファイルの特徴量を算出
S4
秘密鍵・公開鍵を生成
S5
秘密鍵で特徴量を暗号化
S6
暗号化した特徴量を
特徴量保持ファイルに保存
S7
文書情報ファイル、動作プログラムファイル、
特徴量保持ファイルをカプセル化
エンド

【図５】

24

<特徴量ファイル>

<特徴量算出情報　アルゴリズム="SHA-1"/>

<動作プログラム１　動作プログラム名＝“文書作成プログラム”
特徴量="8KBDi/AdAonBKtuztspftk4t/qc="

<動作プログラム２　動作プログラム名＝“文書閲覧プログラム”
特徴量="8KBDi/setasetutwetsptaett/qc="

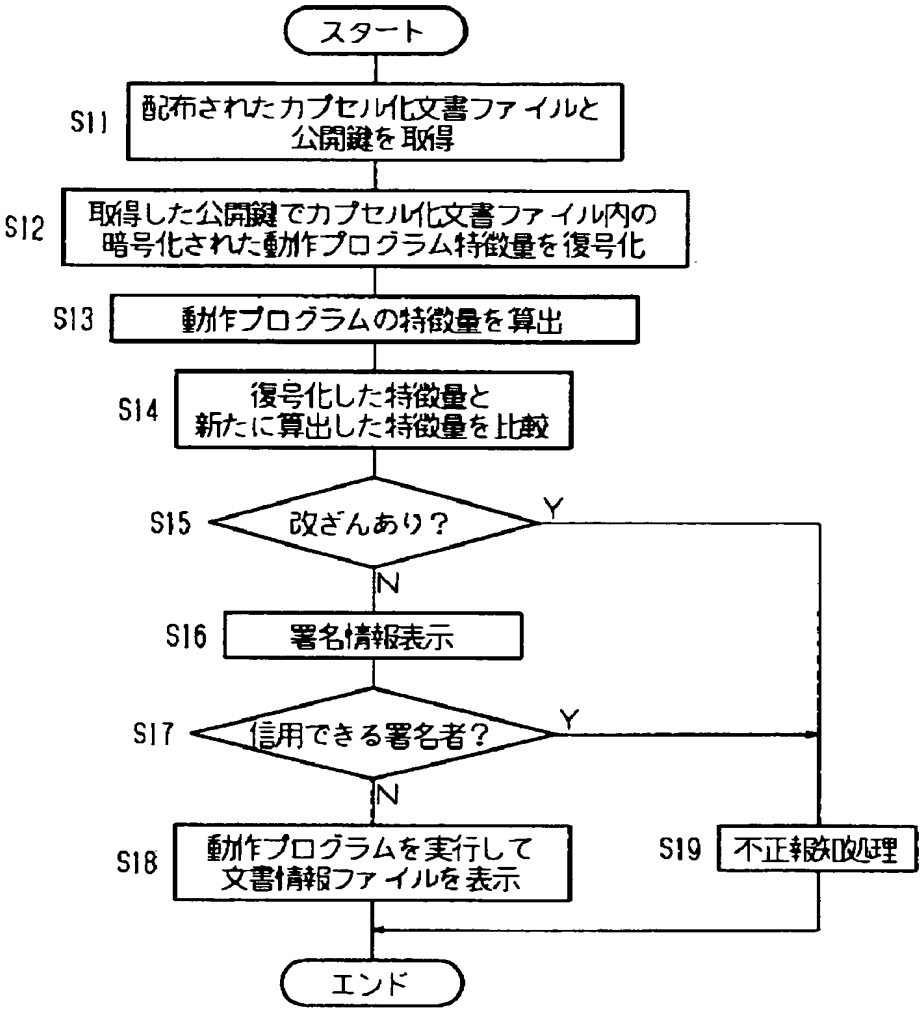
<動作プログラム３　動作プログラム名＝“動作検証プログラム”
特徴量="8KBDi/tajeiue4tuztspfetset/qc="

⋮

<動作プログラム１０　動作プログラム名＝“音楽再生プログラム”
特徴量="8KBDi/AderetstKtuztsfetsfy/qc="

</特徴量ファイル>

【図６】



【図７】

動作権限の種類	動作権限モード				
	A	B	C	D	
カプセル化文書内のファイルの読込み	×	○	○	○	
コンピュータ内のファイルの読込み	×	×	○	○	
カプセル化文書内のファイルの読み書き	×	×	×	○	----------
コンピュータ内のファイルの読み書き	×	×	×	×	
ネットワークのパケットの受信	×	×	×	×	
ネットワークのパケットの送信	×	×	×	×	
⋮					

【図８】

24

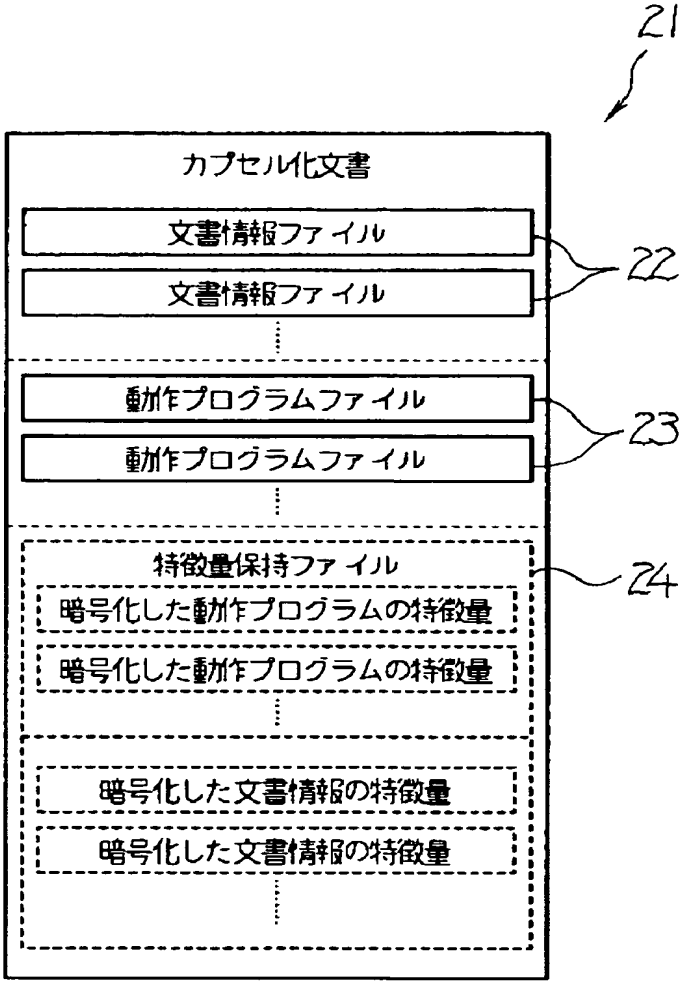
```
<特徴量ファイル>

    <特徴量算出情報　アルゴリズム="SHA-1"/>

    <動作プログラム１　動作プログラム名="文書作成プログラム"
        特徴量="8KBDi/AdAonBKtuztspftk4t/qc="
        公開鍵情報="adklsad49SSDgms"/>

    <動作プログラム２　動作プログラム名="文書閲覧プログラム"
        特徴量="8KBDi/setasetutwetsptaett/qc="
        公開鍵情報="SBSdatajsDgms4g"/>

    <動作プログラム３　動作プログラム名="動作検証プログラム"
        特徴量="8KBDi/tajeiue4tuztspfetset/qc="
        公開鍵情報="www.xxxxx.co.jp/location3/Key/"/>

                        ⋮

    <動作プログラム１０　動作プログラム名="音楽再生プログラム"
        特徴量="8KBDi/AderetstKtuztsfetsfy/qc="
        公開鍵情報="rttszrgrgklsadees3"/>

</特徴量ファイル>
```

【図９】

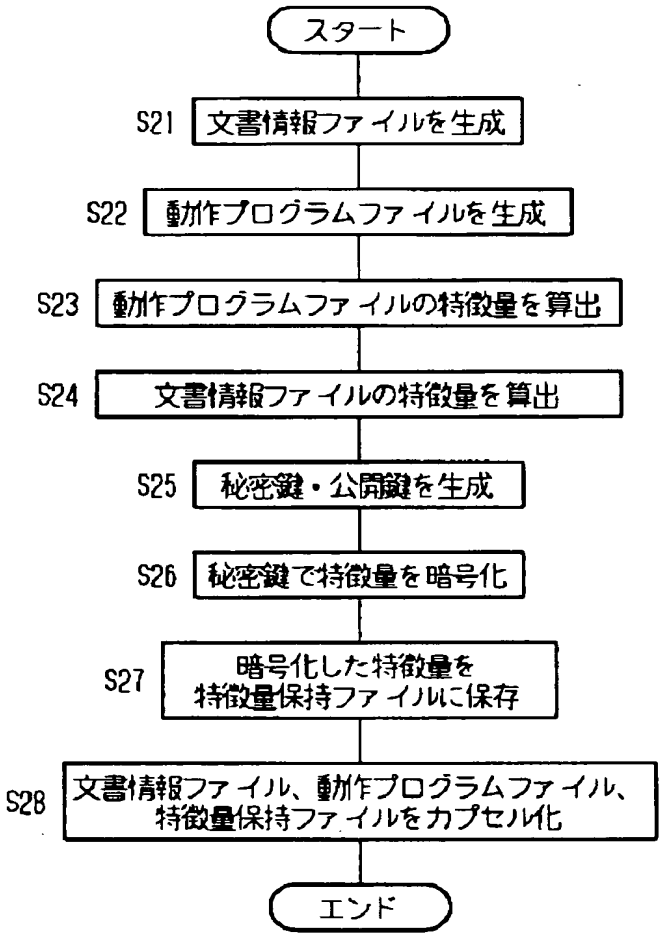
24

```
<特徴量ファイル>

    <特徴量算出情報　アルゴリズム="SHA-1"/>

    <動作プログラム１　動作プログラム名＝“文書作成プログラム”
        位置情報="www.xxxxx.co.jp/location1/"
        特徴量="8KBDi/AdAon8Ktuztspftk4t/qc="
        公開鍵情報="adklsad49SSDgms"/>

    <動作プログラム２　動作プログラム名＝“文書閲覧プログラム”
        位置情報="www.xxxxx.co.jp/location2/"
        特徴量="8KBDi/setasetutwetsptaett/qc="
        公開鍵情報="S8SdatajsDgms4g"/>

    <動作プログラム３　動作プログラム名＝“動作検証プログラム”
        位置情報="www.xxxxx.co.jp/location3/"
        特徴量="8KBDi/tajeiue4tuztspfetset/qc="
        公開鍵情報="www.xxxxx.co.jp/location3/Key/"/>

                    ⋮

    <動作プログラム１０　動作プログラム名＝“音楽再生プログラム”
        位置情報="www.xxxxx.co.jp/location10/"
        特徴量="8KBDi/AderetstKtuztsfetsfy/qc="
        公開鍵情報="rttszrgrgklsadees3"/>

</特徴量ファイル>
```

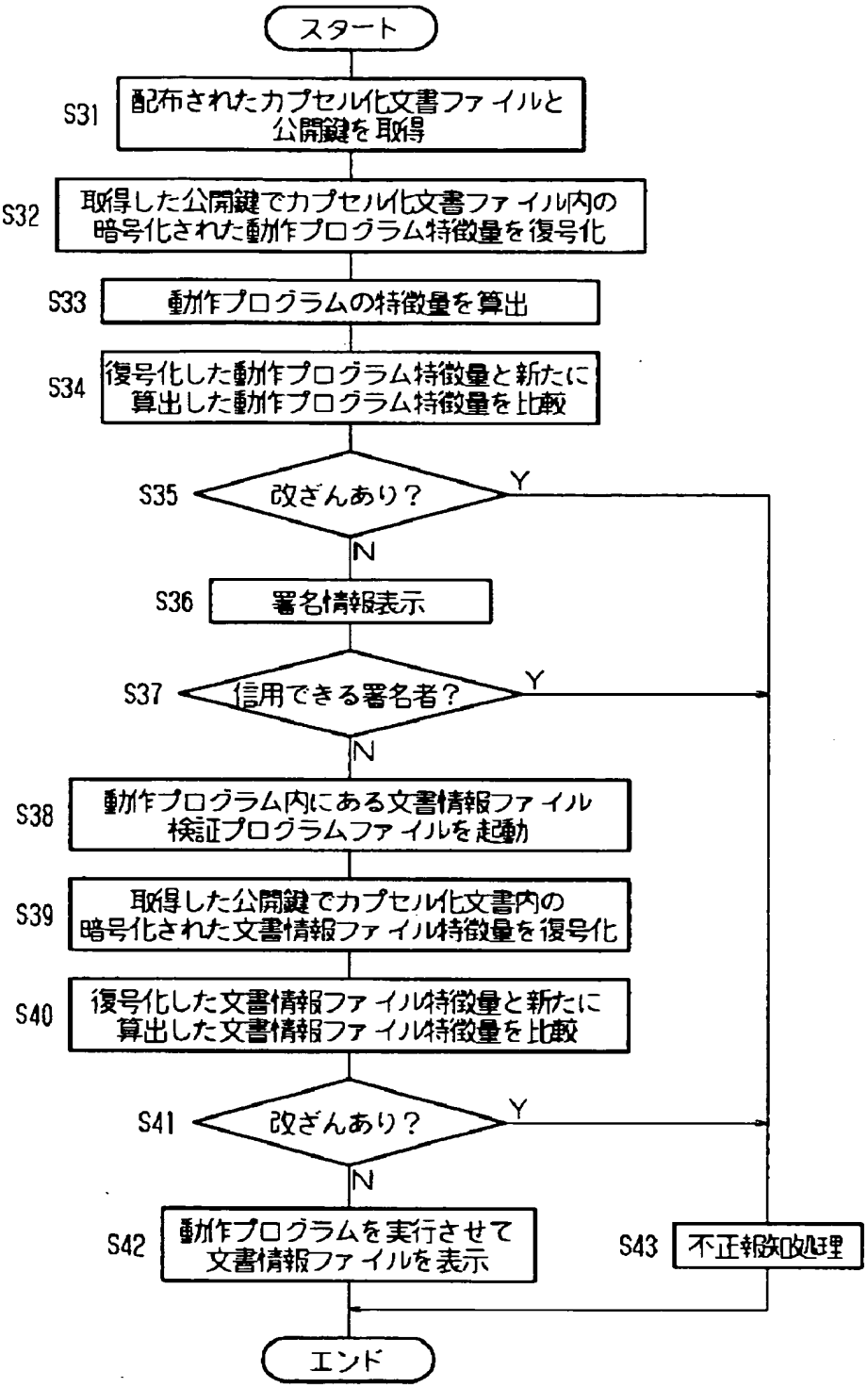
【図１０】


21
カプセル化文書
文書情報ファイル
文書情報ファイル
22
動作プログラムファイル
動作プログラムファイル
23
特徴量保持ファイル
暗号化した動作プログラムの特徴量
暗号化した動作プログラムの特徴量
24
暗号化した文書情報の特徴量
暗号化した文書情報の特徴量

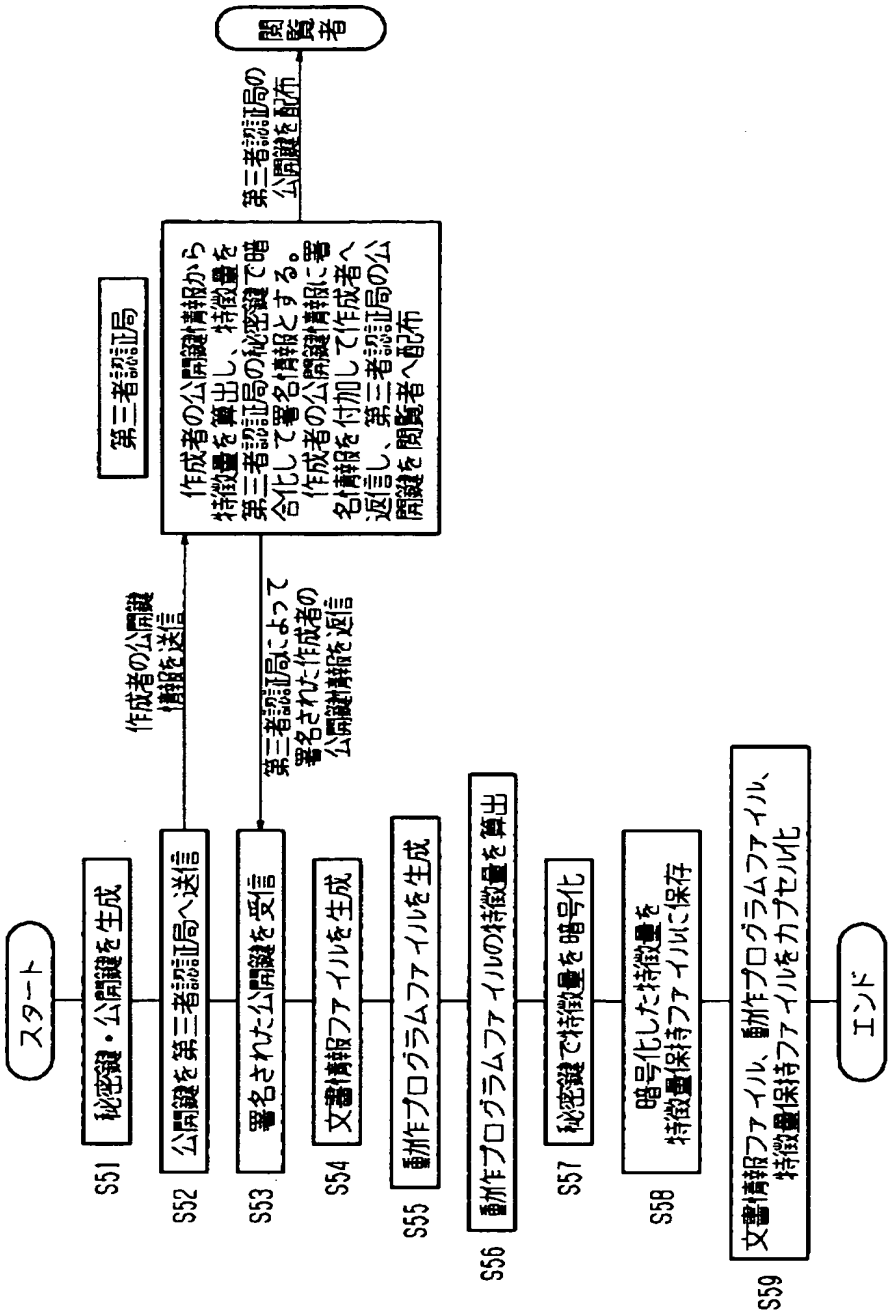
【図１１】


スタート
S21
文書情報ファイルを生成
S22
動作プログラムファイルを生成
S23
動作プログラムファイルの特徴量を算出
S24
文書情報ファイルの特徴量を算出
S25
秘密鍵・公開鍵を生成
S26
秘密鍵で特徴量を暗号化
S27
暗号化した特徴量を
特徴量保持ファイルに保存
S28
文書情報ファイル、動作プログラムファイル、
特徴量保持ファイルをカプセル化
エンド

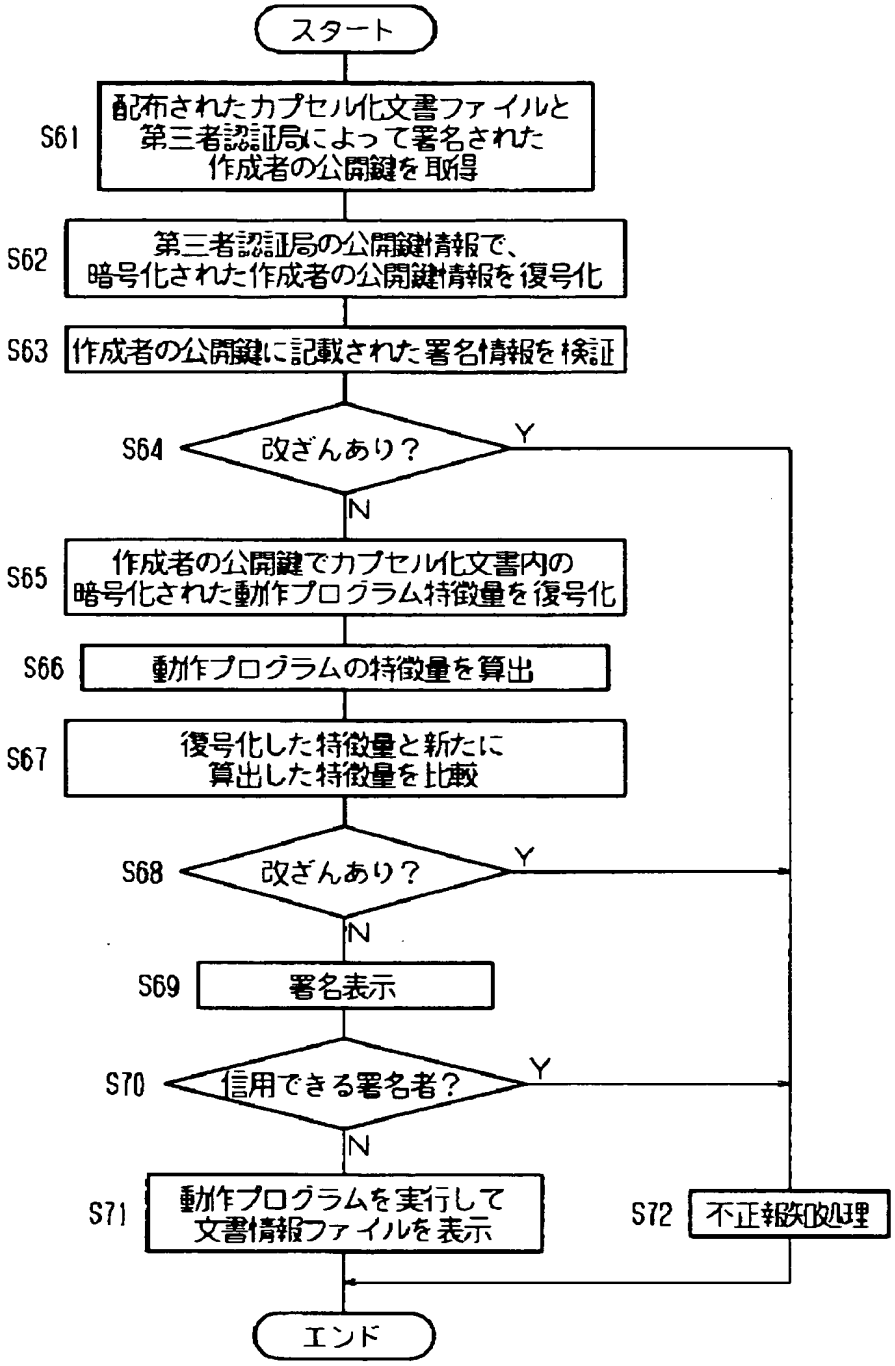
【図１２】


スタート
S31
配布されたカプセル化文書ファイルと公開鍵を取得
S32
取得した公開鍵でカプセル化文書ファイル内の暗号化された動作プログラム特徴量を復号化
S33
動作プログラムの特徴量を算出
S34
復号化した動作プログラム特徴量と新たに算出した動作プログラム特徴量を比較
S35
改ざんあり？
Y
N
S36
署名情報表示
S37
信用できる署名者？
Y
N
S38
動作プログラム内にある文書情報ファイル検証プログラムファイルを起動
S39
取得した公開鍵でカプセル化文書内の暗号化された文書情報ファイル特徴量を復号化
S40
復号化した文書情報ファイル特徴量と新たに算出した文書情報ファイル特徴量を比較
S41
改ざんあり？
Y
N
S42
動作プログラムを実行させて文書情報ファイルを表示
S43
不正報知処理
エンド

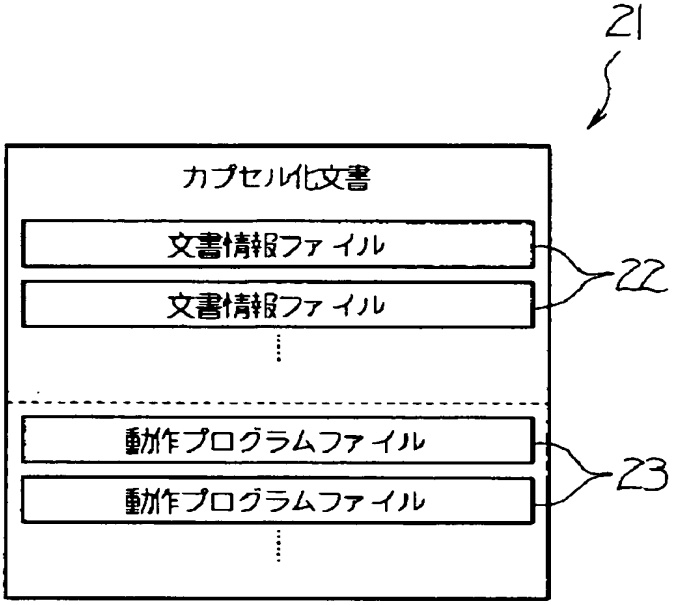
【図１３】


スタート
S51
秘密鍵・公開鍵を生成
S52
公開鍵を第三者認証局へ送信
作成者の公開鍵情報を送信
第三者認証局
S53
署名された公開鍵を受信
第三者認証局によって署名された作成者の公開鍵情報を返信
S54
文書情報ファイルを生成
S55
動作プログラムファイルを生成
S56
動作プログラムファイルの特徴量を算出
S57
秘密鍵で特徴量を暗号化
S58
暗号化した特徴量を特徴量保持ファイルに保存
S59
文書情報ファイル、動作プログラムファイル、特徴量保持ファイルをカプセル化
エンド
作成者の公開鍵情報から特徴量を算出し、特徴量を第三者認証局の秘密鍵で暗号化して署名情報とする。作成者の公開鍵情報に署名情報を付加して作成者へ返信し、第三者認証局の公開鍵を閲覧者へ配布
第三者認証局の公開鍵を配布
閲覧者

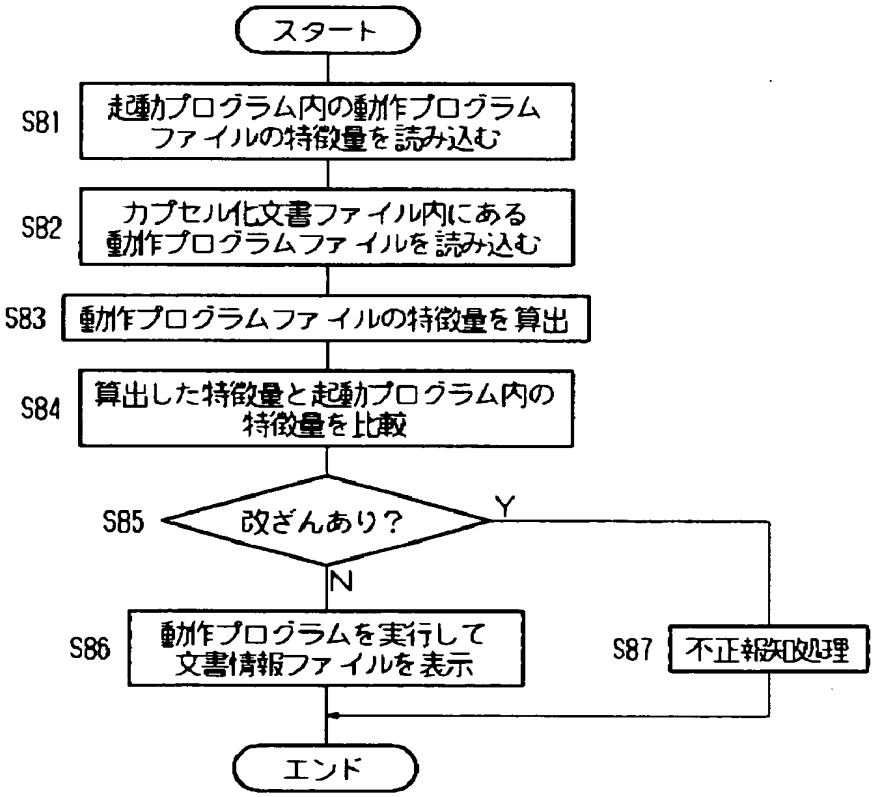
【図１４】


スタート
S61
配布されたカプセル化文書ファイルと第三者認証局によって署名された作成者の公開鍵を取得
S62
第三者認証局の公開鍵情報で、暗号化された作成者の公開鍵情報を復号化
S63
作成者の公開鍵に記載された署名情報を検証
S64
改ざんあり？
Y
N
S65
作成者の公開鍵でカプセル化文書内の暗号化された動作プログラム特徴量を復号化
S66
動作プログラムの特徴量を算出
S67
復号化した特徴量と新たに算出した特徴量を比較
S68
改ざんあり？
Y
N
S69
署名表示
S70
信用できる署名者？
Y
N
S71
動作プログラムを実行して文書情報ファイルを表示
S72
不正報知処理
エンド

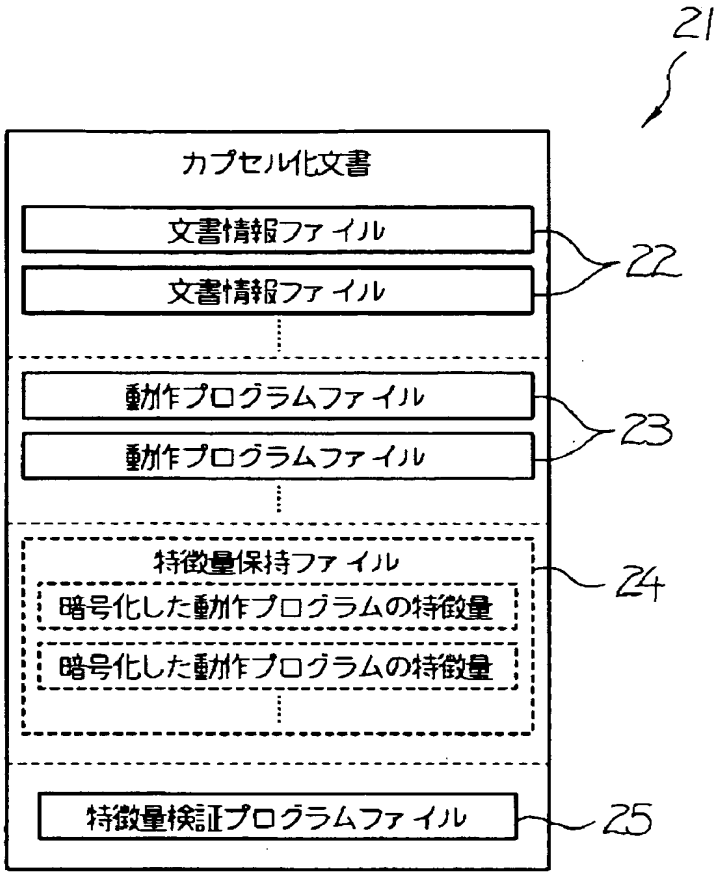
【図１５】


21
カプセル化文書
文書情報ファイル
文書情報ファイル
22
動作プログラムファイル
動作プログラムファイル
23

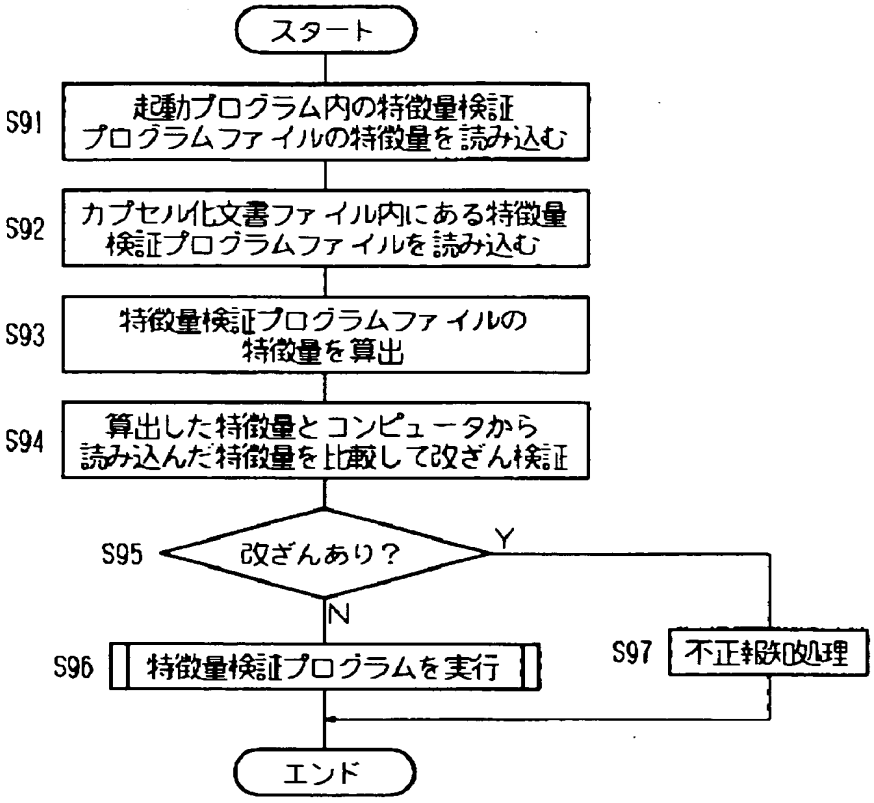
【図１６】


スタート
S81
起動プログラム内の動作プログラム
ファイルの特徴量を読み込む
S82
カプセル化文書ファイル内にある
動作プログラムファイルを読み込む
S83
動作プログラムファイルの特徴量を算出
S84
算出した特徴量と起動プログラム内の
特徴量を比較
S85
改ざんあり？
Y
N
S86
動作プログラムを実行して
文書情報ファイルを表示
S87
不正報知処理
エンド

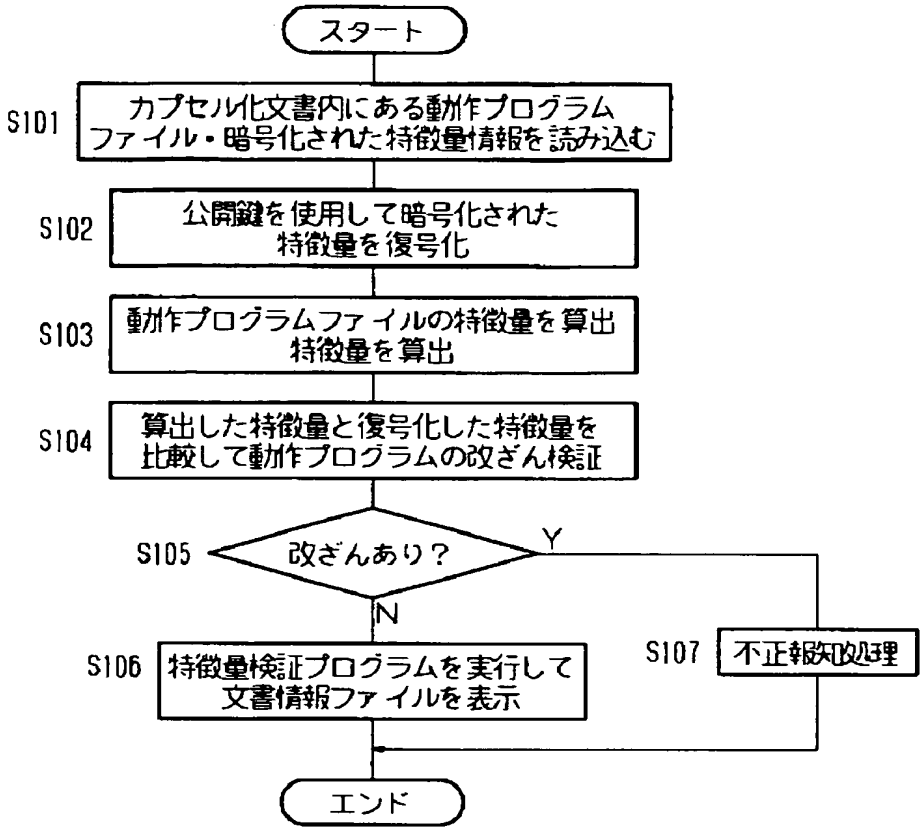
【図１７】


21
カプセル化文書
文書情報ファイル
文書情報ファイル
22
動作プログラムファイル
動作プログラムファイル
23
特徴量保持ファイル
暗号化した動作プログラムの特徴量
暗号化した動作プログラムの特徴量
24
特徴量検証プログラムファイル
25

【図１８】


スタート
S91
起動プログラム内の特徴量検証
プログラムファイルの特徴量を読み込む
S92
カプセル化文書ファイル内にある特徴量
検証プログラムファイルを読み込む
S93
特徴量検証プログラムファイルの
特徴量を算出
S94
算出した特徴量とコンピュータから
読み込んだ特徴量を比較して改ざん検証
S95
改ざんあり？
Y
N
S96
特徴量検証プログラムを実行
S97
不正検知処理
エンド

【図１９】


スタート
S101
カプセル化文書内にある動作プログラム
ファイル・暗号化された特徴量情報を読み込む
S102
公開鍵を使用して暗号化された
特徴量を復号化
S103
動作プログラムファイルの特徴量を算出
特徴量を算出
S104
算出した特徴量と復号化した特徴量を
比較して動作プログラムの改ざん検証
S105
改ざんあり？
Y
N
S106
特徴量検証プログラムを実行して
文書情報ファイルを表示
S107
不正報知処理
エンド

【書類名】　要約書

【要約】

【課題】　コンピュータの動作環境に左右されず、かつ、悪意のあるプログラムの混入を防止できる文書構造を提供する。

【解決手段】　文書上での表現実体となるコンテンツ情報である文書情報ファイル２２と、この文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイル２３と、この動作プログラムファイル２３に関する暗号化された特徴量を保持する特徴量保持ファイル２４と、をカプセル化手段によってカプセル化する。これにより、作成者のコンピュータと異なる環境でも当該文書を閲覧することができ、この際、特徴量保持ファイル２４に保持されている動作プログラムファイル２３の暗号化特徴量を復号化するとともに配布された動作プログラムファイル２３の特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイル２１の配布途中における動作プログラムファイルの改ざん検証ができる。

【選択図】　図３

特願２００３－１９５６２６

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー